March 31, 2009

Health Information Security and Privacy Collaboration

Master Document of Grouped Contract Provisions

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Interorganizational Agreements Collaborative
Alaska, Guam, Iowa, New Jersey, North Carolina, South Dakota

Health Information Security & Privacy
COLLABORATION

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

March 31, 2009

Health Information Security and Privacy Collaboration

Master Document of Grouped Contract Provisions

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Interorganizational Agreements Collaborative
Alaska, Guam, Iowa, New Jersey, North Carolina, South Dakota

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 USC. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

CONTENTS

Section **Page**

TABLES

1. INTRODUCTION

From the beginning of Phase III, the Interorganizational Agreements (IOA) Collaborative recognized the value of work completed in earlier phases of the Health Information Security and Privacy Collaboration (HISPC), along with the value of work completed by other health information exchange entities. As a result, one of the first steps of the IOA Collaborative was to gather a starter set of existing agreements and/or contracts developed or currently used to support electronic health information exchange. The documents collected included data sharing agreements (DSAs), memoranda of understanding (MOUs), participant agreements, policies, presentations, and white papers from a wide variety of sources such as HISPC states, private and public health care entities, health care attorneys, and national projects such as the Nationwide Health Information Network (NHIN) Data Use and Reciprocal Support Agreement (DURSA) Workgroup and Integrating the Healthcare Enterprise (IHE). A total of 48 documents were collected and included in the Documents Library of Data Sharing Agreements (the "Library"—a list is included below).

The content of the Library documents ranges from general guidelines and model language, as in the Markle Foundation Model Contract for Health Information Exchange, to very specific legal language for exchanges of limited categories of information, as in the Biosurveillance Data Use Agreement. These documents were obtained from many different sources, and IOA Collaborative members sought approval to use and reference the documents in ongoing IOA Collaborative work.

In addition to seeking approval for the IOA Collaborative's internal use of the documents, each source organization was asked for permission to make some or all of its agreement publicly available as part of the Classification Scheme described in Section 3. Because the IOA Collaborative deliverables will be publicly available, approval from the sources was necessary to the extent that any of the language could be directly attributed to a particular organization and/or was proprietary or confidential. The IOA Collaborative found that most organizations were extremely cooperative and generous in sharing the language contained in their documents. However, a few documents were not approved for public release. Those documents not approved were removed from the Library after internal workgroup analysis (see Section 2 for a list of documents). The Library was useful as a drafting tool for the IOA Collaborative during the development process and will remain useful going forward as reference material for those involved in electronic health information exchange.

Once the Library was created, the IOA Collaborative's next task was to review, break down, and categorize the sections contained in each document for comparison to other, similar provisions. To accomplish this, the IOA Collaborative had to develop a relatively straightforward method for categorization that could be applied by all members. The IOA North Carolina team devised a system called the "Classification Scheme" that allowed each document to be divided and labeled by document source, document identifier, document type, subject matter, page or section, and general category or subcategory of information. An example of the Classification Scheme is provided in Section 3.

This scheme was used to classify all provisions from the applicable documents in the IOA Library as follows: The 48 documents in the Library were divided among the IOA Collaborative member states for classification. The classifications were submitted back to the IOA Collaborative and compiled into a Master Document of Grouped Contract Provisions (included in Section 4), a document used to strike provisions that conflicted with individual state laws, rank the provisions according to preferred language, and create model language for the agreements. This document contained all of the substantive provisions from the most applicable documents, carefully labeled using the Classification Scheme. However, because some source documents were not approved for public release, the Master Document of Grouped Contract Provisions included here has been stripped of all primary identifiers to protect the source of the agreements (i.e., all codes pertaining to document source, document identifiers, and page or section references were removed). As a result, the Classification Scheme included with this deliverable is shorter than the one presented in the IOA Collaborative's final report.[1]

The sequential process of using the Library, the Classification Scheme, and the Master Document of Grouped Contract Provisions enabled the IOA Collaborative to choose the most applicable and preferred contract language for model cross-state data sharing agreements without drafting the agreements from scratch.

[1] See the Interorganizational *Agreements Collaborative Final Report* to review the more detailed Classification Scheme used by the Collaborative.

2. IOA DOCUMENTS LIBRARY OF DATA SHARING AGREEMENTS

IOA reviewed and analyzed the following publicly available DSAs. These agreements are included in the IOA Documents Library of Data Sharing Agreements.

1) All Women Count! Participating Clinic Agreement. This agreement is a form agreement, provided by the named program within the South Dakota Department of Health, between a state agency and a clinic participant to participate in screening exams.

2) Fundamentals of the Electronic Medical Record. This document is a PowerPoint presentation developed for the American Health Lawyers Association.

3) The Indiana Network for Patient Care: A Case Study of a Successful Healthcare Data Sharing Agreement. This white paper, authored by Sears, Prescott, and McDonald, describes the creation and evolution of the Indiana Network for Patient Care and analyzes the agreement listed in item #35 below.

4) "Getting Connected with caBIG" Data Sharing and Security Framework. This document is from the Cancer Biomedical Informatics Grid of the National Cancer Institute.

5) HISPC Communications Plan for the State of Alaska. This document is self-explanatory.

6) Alaska Chartlink Form Identification and Authorization Verification Policy and Procedure. This document is a policy addressing identification and authorization for the Alaska Chartlink, a statewide regional health information organization (RHIO) composed of public and private providers and payers.

7) Alaska Chartlink Patient Participation Agreement. This document is an agreement to be entered into between individual patients and Alaska Chartlink.

8) Alaska Chartlink Policies and Procedures for Addressing Breaches of Confidentiality. This document is a policy of Alaska Chartlink for the protection of health information and to address breaches of confidentiality.

9) Alaska Chartlink Privacy and Confidentiality Policy. This document is another policy of Alaska Chartlink that specifically addresses privacy of protected health information.

10) Alaska Chartlink Provider Participant Agreement. This document is a form agreement to be executed between individual providers and Alaska Chartlink.

11) Agreement between the Gila River Indian Community and the Arizona Department of Health Services. This document, posted on the Centers for Disease Control and Prevention (CDC) website, provides for the exchange of clinical and public health information between the parties.

12) Introduction to the Laws Governing Formation of Cross-Border Agreements by the States and Generic Public Health Annex. This draft briefing paper was prepared by the employees of the Association of State and Territorial Health Officials and addresses agreements with entities outside the United States.

13) Data Use Agreement. This document is a form agreement used by the Centers for Medicare & Medicaid Services (CMS) and those users to whom it discloses data files.

14) Biosurveillance Data Use Agreement Limited Edata Sets for System Testing. This document is an agreement created by John R. Christiansen, Christiansen IT Law, in Seattle, WA, for researchers and data providers regarding a biosurveillance program.

15) caBIG DSIC WS Datasharing Framework. This document is a visual description of a sharing framework to be utilized to evaluate the sensitivity of data to be shared and identifying conditions, limitations, and restrictions on such sharing of data from the Cancer Biomedical Informatics Grid of the National Cancer Institute.

16) caBIG Datasharing Plan Content Guideline. This document sets out information about the sharing of data within the Cancer Biomedical Informatics Grid of the National Cancer Institute.

17) Health Information Institute Insurance Company Information Reporting Agreement. This document is a form agreement of The Health Information Institute, a Washington corporation, to be entered into between The Health Information Institute, which serves as an HIE, and individual insurance companies.

18) Health Information Institute Provider Financial Responsibility Agreement. This document is a form agreement to be entered into between the Health Information Institute and an entity for access to childhood immunization information contained in a relevant immunization registry and tracking system for the access to such information by individual providers.

19) Health Information Institute Healthcare Provider Information Sharing Agreement. This document is a form agreement between the Health Information Institute and individual providers (as opposed to larger entities), but which may include professional corporations or other entities that employ providers, for the sharing of information within the HIE.

20) Health Information Institute Individual Healthcare Provider Information Sharing Agreement. This document is a form agreement to be entered into between the Health Information Institute and individuals (but not entities) who are licensed to provide health care. The agreement is for the sharing of data within the HIE.

21) Oklahoma State Department of Health (OSDH)/Oklahoma State Immunization System (OSIIS) Facility Authorization Request.

22) Public Health Data Sharing Agreement. This document is a form agreement for the sharing of public health-related data to be entered into among the Michigan Department of Community Health, Minnesota Department of Health, New York State Department of Health, Province of Ontario, and the Wisconsin Department of Health and Family Services.

23) Template for a Comprehensive Health Care Information Protection Agreement between Business Associates. This document is a template for agreements providing for the protection of health information in the course of electronic

transactions among health care organizations. The template was originally presented by the Health Key Collaborative; principal author, John R. Christiansen.

24) Health Information Exchange Data User Agreement. This form agreement is to be entered into between a data user and a network for a data user to have privileges within a health information exchange. The document does not contain identifying information as it was provided confidentially and anonymously.

25) Health Information Exchange Hospital Agreement. This document is a form health information exchange agreement between a network and a hospital for the hospital to participate in the health information exchange. This agreement also was provided by an anonymous source.

26) Health Information Exchange Policies and Procedures. This document contains form policies and procedures to be utilized by an HIE. The network is again anonymous.

27) IHE IT Infrastructure Technical Framework White Paper. Provided by ACC/HIMSS/RSNA, this document is a white paper addressing technical frameworks for an HIE infrastructure. The paper addresses issues to consider when planning the deployment of XDS Affinity Domains, defines the areas of the XDS and related profiles to consider refining for XDS Affinity Domains, and provides a standardized document template to be used when specifying the deployment policies for a single XDS Affinity Domain or for multiple XDS Affinity Domains in a particular nation or geographic region.

28) Oklahoma State Department of Health (OSDH)/Oklahoma State Immunization Information System (OSIIS) User Authorization Request.

29) Iowa Immunization Registry Information System (IRIS). This document is an agreement provided by the Iowa Department of Public Health to be executed by medical practices, health maintenance organizations (HMOs), health departments, clinics, and other entities wishing to participate in IRIS.

30) Kids Immunization Database/Tracking System (KIDS) Registry Security and Confidentiality Agreement. This agreement of the Philadelphia Department of Public Health Immunization Program is to be entered into with organizations such as health care entities or schools that are given access to a public health registry.

31) Key Topics in a Model Contract for Health Information Exchange. This and the next document are part of the Connecting for Health Common Framework, provided by the Markle Foundation, which address model terms and conditions for "sub-network organization" entities to provide information within an HIE.

32) A Model Contract for Health Information Exchange. This and the previous document are part of the Connecting for Health Common Framework, provided by the Markle Foundation, which addresses model terms and conditions for "sub-network organization" entities to provide information within an HIE.

33) Draft Memorandum of Agreement between the New Jersey Department of Health and Senior Services and New York City Department of Health and Mental Hygiene through the New York State Department of Health, Center for Community Health, Office of Health Systems, for a Pilot Test of the New Jersey-New York City Health

Datashare Project. This document is a draft memorandum of agreement for the sharing of health care data between New Jersey and New York City.

34) New Mexico Health Information Collaborative Subscription Agreement. This document is an agreement to be entered into between the Loveless Clinic Foundation and participants within the collaborative. The agreement grants a nontransferable license to the participant for access and use of the software applications relating to the collaborative.

35) Indiana Network for Patient Care Second Participants' Agreement. This revised agreement allows the participants in the Indiana Network for Patient Care to share information for purposes of emergency room and primary care as well as research purposes.

36) Health Information Exchange Agreement. This agreement is a form health information exchange agreement drafted by the North Carolina Healthcare Information and Communication Alliance as part of its deliverables under the HISPC project.

37) State of South Dakota Memorandum of Understanding for the South Dakota Immunization Information System. This memorandum of understanding is a form agreement to be entered into between the State of South Dakota and an individual clinic for participation within the South Dakota Immunization Information System.

38) The Regents of the University of Michigan. This document is a data use agreement between the Regents on behalf of the University of Michigan Health System and individual entities for access to a limited data set for purposes of research, public health, or operations.

39) Guidelines for U.S.-Mexico Coordination on Epidemiologic Events of Mutual Interest. This document, posted on the CDC website, was produced by the Core Group on Epidemiologic Surveillance and Information Sharing Health Working Group, U.S.-Mexico Binational Commission.

40) Research Agreement between Iowa Department of Public Health and [Insert Party Here]. This document is a form agreement utilized by the Iowa Department of Public Health and individual researchers whereby the Iowa Department of Public Health agrees to release to the researcher vital statistic records requested in the application of the researcher. The researcher then agrees to use such records for bona fide research purposes.

IOA reviewed and analyzed the following proprietary DSAs. Because of their proprietary status, these Agreements are not included in the IOA Documents Library of Data Sharing Agreements.

41) Colorado Regional Health Information Organization Participant Registration Agreement. This agreement is to be entered into between the Colorado Regional Health Information Organization and Kaiser Foundation Hospitals. The agreement registers the Kaiser Foundation Hospitals as participants within the Colorado Regional Health Information Organization.

42) Data Use and Reciprocal Support Agreement (DURSA). This agreement is the June 2008 version for the participants within the NHIN for the exchange of TEST data

only. This version of the DURSA was not yet approved for public sharing. However, the IOA also reviewed the final test data DURSA when it was approved and that version is included in the Library (see item #47 below).

43) Colorado Regional Health Information Organization Participant Registration Agreement. This document is an agreement entered into between the Colorado Regional Health Information Organization and the Children's Hospital Association for the Children's Hospital Association to be a participant within the Colorado Regional Health Information Organization. This agreement appears to be somewhat different than the Colorado Regional Health Information Organization Agreement entered into with the Kaiser Foundation Hospitals.

IOA received the following publicly available DSAs after the submission deadline. These agreements were reviewed but were not included in IOA's analysis. These agreements are included in the IOA Documents Library of Data Sharing Agreements.

44) All Women Count! Participating Hospital Agreement. This agreement is a form agreement, provided by the named program within the South Dakota Department of Health, between a state agency and a hospital participant.

45) Business Associate Addendum. This document contains a template for business associate addendums to HIE agreements. The network is again anonymous.

46) Amended and Restated Clinical Outcomes Assessment Program Health Care Provider Information Sharing Agreement. This document is a form agreement between the Foundation for Healthcare Quality, which collects and analyzes cardiac care clinical outcomes information, and participants within the Clinical Outcomes Assessment Program cardiac registry. The agreement allows such participants to share information within the registry.

47) Data Use and Reciprocal Support Agreement (DURSA). This agreement is the executable test data DURSA developed for participants in the NHIN dated 8/26/08. This version of the DURSA is approved for public sharing.

48) HIE Developer Corporation Information Exchange Infrastructure Development Agreement. This document is a template for agreements pertaining to HIE technology infrastructure development. The agreement was prepared by John R. Christiansen.

3. CLASSIFICATION SCHEME

Provisions of agreements or portions of other documents are labeled in accordance with the following classification scheme[2]:

_ _._ _/	_ _._ _/	(_ _)-	_ _._ _
Document Identifier	Document Type. Subject Category	Page or Section	Provision Category

Each space represents an alpha numeric character (listed below) that represents the following:

Document Type . Subcategory of Document Type Regarding Subject Matter of Document – General Category of Provision . Subcategory of the General Category of Provision

Sample Complete Reference: Using the reference information in Tables 3-1, 3-2, and 3-3, a provision defining the term "Authorized User" would be referenced as "hh.06-DE.01" wherein "hh" references the document type (HIE to HIE), "06" references the subject matter of the document (general data sharing, not specific), "DE" indicates this is a definition, and "01" refers to the term "Authorized User."

Table 3-1. Document Type

Code	Document Type
ss	State to state
sp	State and private
pp	Private to private
ph	Private to HIE
hh	HIE to HIE
mm	Miscellaneous (policies & procedures, presentations, etc.)

Table 3-2. Subject Matter of Document

The following subcategories explain the subject matter of each document. For instance, an agreement for the exchange of immunization data between state agencies would be labeled "ss.08."

Code	Subcategories
01	Business associate agreements
02	Clinical outcomes reporting and research generally
03	Diagnostic screening
04	General educational
05	General data sharing specific to public health areas
06	General data sharing; not specific to a particular field or specialty
07	Identification, verification, and authorization of user
08	Immunization
09	Overall strategy/plan
10	Technical/infrastructure descriptions/overviews

[2] See the *Interorganizational Agreements Collaborative Final Report* to review the more detailed classification scheme used by the Collaborative.

Table 3-3. Contract/Document Provision Categories/Subcategories

Note: Capitalized terms in quotations are samples of the defined terms described by each particular subcategory. Some agreements may use similar but different defined terms. Defined terms are not used in the descriptions of any of the categories or subcategories. Defined terms used in a particular section other than the definitions section should be included in such substantive section (e.g., "applicable law" should be included in "BP.01"). The descriptions provided are intended to be as broad as possible.

Code	Categories/Subcategories
DE	**Definitions**
DE.01	"Authorized User"; an individual designated to use the services provided by the HIE on behalf of the participating party
DE.02	"Data Provider"; a participant registered to provide information to the HIE
DE.03	"Data Recipient"; a participant that obtains information from the HIE
DE.04	HIPAA
DE.05	"Participant"; provides data to and/or receives data from the HIE
DE.06	"Participant Type"; health care industry classification of a participant
DE.07	"Data"; electronic information provided to the HIE
DE.08	"Agreement"; registration agreement with the HIE
DE.09	"Services"; services provided by the HIE
DE.10	"Network"; the HIE's system that allows for peer-to-peer communication/transfer of data
DE.11	Miscellaneous
RE	**Recitals**
RE.01	Description of HIE
RE.02	Description of non-HIE party
RE.03	Statement of purposes of the agreement
RE.04	Miscellaneous
SR	**Statement of Relationship**
SR.00	CLASSIFICATION FILLER—NO SUBCATEGORIES
RR	**Data Recipient Requirements/Limitations (requirements that apply specifically to recipients of data)**
RR.01	Acceptance of grant of right/license to use the HIE
RR.02	Acceptance of compliance with other policies/procedures adopted by the HIE (current and future)
RR.03	Scope of use of services available to recipient
RR.04	Prohibitions on recipient's use of data
RR.05	Ensuring compliance with applicable laws
RR.06	Obligation to obtain and maintain compliant software/hardware necessary to utilize the HIE
RR.07	Miscellaneous
PR	**Data Provider Requirements/Limitations (requirements that apply specifically to providers of data)**
PR.01	Acceptance of grant of right/license to use the HIE
PR.02	Acceptance of compliance with other policies/procedures adopted by the HIE (current and future)
PR.03	Format of data
PR.04	Connection to network
PR.05	Accuracy of data provided
PR.06	Timely provision of data

Code	Categories/Subcategories
PR.07	Completeness of data
PR.08	Grant of right/license to the HIE (and its users) to access the data provided; including limitations on use
PR.09	Compliance with applicable law
PR.10	Obligation to obtain and maintain compliant software/hardware necessary to utilize the HIE
PR.11	Training of employees/agents
PR.12	Miscellaneous
SH	**Software/Hardware (provided by the HIE)**
SH.01	Description of software/hardware provided
SH.02	Grant of right/license to receiver of software/hardware
SH.03	Limitations on copying software and other requirements relating to copying software
SH.04	Restriction/prohibition on modification of software
SH.05	Covenant to execute all licensing or other agreements required by third-party vendors
SH.06	Miscellaneous
PY	**Privacy**
PY.01	Compliance with HIPAA privacy generally
PY.02	Compliance with state law
PY.03	Breach of confidentiality (improper use of data)
PY.04	Business associate
PY.05	Use of protected health information
PY.06	Agents/subcontractors of the participant
PY.07	Access to PHI; right to inspect and copy
PY.08	Amendment of PHI
PY.09	Reports of disclosure of PHI
PY.10	Availability of records to HHS
PY.11	Survival of privacy provisions after termination of agreement with the HIE
PY.12	Miscellaneous
SE	**Security**
SE.01	Compliance with HIPAA security generally
SE.02	Breach of security
SE.03	Administrative safeguards
SE.04	Technical safeguards
SE.05	Physical safeguards
SE.06	Agents/subcontractors of the participant
SE.07	Miscellaneous
TT	**Term and Termination**
TT.01	Term
TT.02	Termination generally
TT.03	Termination for cause
TT.04	Termination without cause
FC	**Fees/Consideration**
FC.01	Fee schedule
FC.02	Payment of fees
FC.03	Change in fees

Code	Categories/Subcategories
FC.04	Additional costs/charges
FC.05	Suspension of service
FC.06	Miscellaneous
CP	**Confidentiality of Proprietary Information**
CP.01	Scope of information covered/definition
CP.02	Scope of allowed/disallowed disclosure
CP.03	Remedies
CP.04	Miscellaneous
DI	**Disclaimers**
DI.01	Disclaimers regarding use of network
DI.02	Disclaimers regarding quality, accuracy, completeness, timing, etc. of services or data
DI.03	Disclaimers regarding action/omission of other participants
DI.04	Disclaimers regarding patient care
DI.05	Disclaimers regarding participant's use of data
DI.06	Limitation on HIE liability
DI.07	Miscellaneous
IN	**Insurance**
IN.01	Participant requirement
IN.02	HIE requirement
IN.03	Miscellaneous
IM	**Indemnification**
IM.01	Indemnification of participant
IM.02	Indemnification of the HIE
IM.03	Participant's indemnification of other participants
IM.04	Miscellaneous
BP	**Boilerplate Contract Provisions/General Contract Provisions**
BP.01	Applicable law
BP.02	Venue; jurisdiction
BP.03	Assignability/nonassignability
BP.04	Third-party beneficiaries
BP.05	Force majeure
BP.06	Severability
BP.07	Notice
BP.08	Waiver
BP.09	Breach
BP.10	Miscellaneous

4. MASTER DOCUMENT OF GROUPED CONTRACT PROVISIONS

4.1 Definitions (DE)

DE.01 Definition of Authorized User

mm.06–DE.01
Authorized Users

User Enrollment

Network member hospitals may enroll:

- Exchange physicians who have staff privileges at an Exchange hospital;
- Those physician's office staff;
- Exchange hospital-employed RNs who are primarily assigned to the Emergency Department ("ED") and Exchange hospital ED physicians;
- Exchange health care providers such as nursing home and health department staff; and
- Exchange hospital-employed licensed clinicians who are performing a dedicated case management role.

(collectively referred to as "Authorized Users") to access electronic patient data through Exchange. The term "physician" as used in this section shall include Doctor of Medicine (MD), Physician Assistant (PA), Nurse Practitioner (NP), Doctor of Osteopathic Medicine (DOM), Doctor of Podiatric Medicine (DPM), Doctor of Dental Surgery (DDS), Doctor of Psychology (PsyD), Certified Nurse Midwife (CNM), residents and Certified Registered Nurse Anesthetist (CRNA).

sp.08–DE.01
Users, defined as anyone with access to the [Immunization] Registry, must read and sign a [Immunization] Registry User Security and Confidentiality Agreement. Users are categorized into one of the following user types:

- Immunization providers (both private and public)
- Health Management Organizations (HMO)
- Public and private schools
- Department of Public Health employees and their authorized agents (e.g., [Immunization] Registry staff)

[IMMUNIZATION PROGRAM NAME] (11/2007). The following table outlines the different types of [Immunization] Registry access allowed for each user group type.

Table 4-1. [Immunization] Registry Access

User Type	View Immunizations	View Demographics	Add/Edit Information
Immunization Providers	•	•	•1
HMO	u	—	—
Schools	u	u	—
[IMMUNIZATION PROGRAM NAME] /Agents	•	•	•

NOTE: • = has authorization to access all information; u= has authorization to access a subset of the information, with contact information removed; 1 = only a subset of immunization providers have access to add or edit information.

ph.06-DE.01
The Model assumes that the Participant will be permitted to select its Authorized Users without review or approval by the SNO. The SNO may, however, wish to adopt specific credentialing criteria for Authorized Users that would be administered by the SNO, and which may, if desired, be set forth in the SNO Terms and Conditions. The Model assumes that Participants will be required to inform the SNO of changes to their lists of Authorized Users on an ongoing basis. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users.

hh.06-DE.01
"Registered User" means employees, contractors and staff of an Authorized User who are allowed access to the Exchanges or to generate Data on an Exchange pursuant to this Agreement.

ph.09-DE.01
"Authorized User" means an individual Participant or an individual designated to use the SNO's Services on behalf of the Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant's medical staff.

ph.06-DE.01
"Authorized User" means an individual Participant or an individual designated to use the Services on behalf of the Participant, including without limitation, an employee of the Participant and/or a credentialed member of the Participant's medical staff.

ph.06-DE.01
The term "Authorized User" is used to identify the individual users of the SNO's Services. Authorized Users would receive their rights to use the SNO's Services either by registering as Participants themselves or through another organization that registers as a Participant and designates individuals who will be authorized to use the SNO's Services on the Participant's behalf. For example, an Authorized User may be an individual physician who registers as a Participant. In addition, an Authorized User may be a member of that physician's office staff designated by the physician, or any one of a number of a hospital's employees and/or medical staff members authorized by the hospital to act as Authorized Users under the hospital's registration as a Participant.

DE.02 Definition of Data Provider

ss.05-DE.02
A "sending signatory" is a signatory to this Agreement which sends or delivers information to the jurisdiction of another signatory.

ph.06-DE.02
"Data Provider" means a Participant that is registered to provide information to [SNO Name] for use through the Services.

ph.06-DE.02
The Model distinguishes between those Participants who provide data to the Network ("Data Providers") and those who use that data ("Data Recipients"). A Participant may be a Data Provider, a Data Recipient, or both. Participants are identified as Data Providers and/or Data Recipients during the registration process (Section 4.1 (Registration Required)). Because the SNO is assumed to operate as a record-locator service-based, peer-to-peer network, and not as a maintainer of health information, the Model does not contemplate that

individuals will register as Data Providers who would add their own health information to the Network. However, an entity providing such a service to individuals could register as a Data Provider under the Model.

ph.09-DE.02
"Data Provider" means a Participant that is registered to provide information to the SNO for use through the SNO's Services.

mm.10-DE-02
A "sending signatory" is a signatory to this Agreement and Annex which sends, delivers or transports people, material or information to within the jurisdiction of another signatory with its permission and/or at its request.

DE.03 Definition of Data Recipient

mm.10-DE-03
A "receiving signatory" is a signatory to this Agreement and Annex which requests, receives and/or accepts people, material or information within its jurisdiction from another signatory.

ph.09-DE.03
"Data Recipient" means a Participant that uses the SNO's Services to obtain health information.

ph.06-DE.03
"Data Recipient" means a Participant that uses the Services to obtain health information.

ss.05-DE.03
A "receiving signatory" is a signatory to this Agreement which collects, uses, or discloses health data from another signatory.

DE.04 Definition of HIPAA

sp.02-DE.04
(vii) Information Protection Law means:

A. The federal Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations ("HIPAA");
B. Any statute, regulation, administrative or judicial ruling, or regulatory guidance applicable to the Participant in the state of the Participant's legal formation, which imposes privacy and/or information protection requirements on the Participant; and
C. Any statute, regulation, administrative or judicial ruling, or regulatory guidance applicable to the Participant in any state in which the Participant has an associated Provider subject to this Agreement, which imposes privacy and/or information protection requirements on the Participant.

ph.06-DE.04
"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated there under at 45 CFR Parts 160 and 164.

mm.06-DE.04
Privacy Rule (or the "Rule") refers to the final regulations regarding the privacy of individually identifiable health information promulgated by the Department of Health and

Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ph.06-DE.04
Privacy Rule. Privacy Rule shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164.

ph.09-DE.04
"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated there under at 45 CFR Parts 160 and 164.

DE.05 Definition of Participant

ss.05-DE.05
A "signatory" is a jurisdiction participating in this Agreement.

ph.06-DE.05
"Participant" means a party that registered with [SNO Name] to act as a Data Provider and/or as a Data Recipient.

ph.06-DE.05
The term "Participant" is used to refer to both Data Providers and Data Recipients.

pp.06-DE.05
Section 1.12 Participants. The term "Participants" shall mean both Storing Participants and Full Participants. Additional Participants may be added under the procedures in Section 11.02.

mm.10-DE-05
"Health care personnel" is any natural person who provides health care services including, but not limited to, dentists, emergency medical personnel, emergency medical technicians, drivers of emergency vehicles, nurses, nurse practitioners, physicians, physician assistants and pharmacists.

ph.09-DE.05
"Participant" means a party that registered with the SNO to act as a Data Provider and/or as a Data Recipient.

DE.06 Definition of Participant Type

ph.09-DE.06
"Participant Type" means the category of Participants to which a particular Participant is assigned based upon that Participant's role in the health care system.

ph.06-DE.06
4.3.2 Participant Type. How the SNO will categorize Participants by their respective roles in the health care system. Each registrant shall register to participate in one of the following Participant Types: (a) Physician or medical group; (b) Laboratory; (c) Hospital; (d) Public health agency; (e) Pharmacy; (f) Pharmacy benefit manager; (g) Health plan, insurer or other payor; (h) Researcher; and (i) [additional or different provider types selected by the SNO, subject to any limits imposed by the Common Framework Policies and Procedures].

DE.07 Definition of Data

ph.06-DE.07
"Data" means any data or information accessible via the Exchange by or on behalf of Hospital or its registered users, including, without limitation, personally identifying information and protected health information.

mm.10-DE.07
Refinement of Further Submission Set Metadata Attributes (example)

Define a sub-section for each remaining Submission Set Metadata Attribute that the XDS Affinity Domain refines the use of. Explain how the value for each of these attributes must be specified. If a defined set of values should be used and this is not defined in the XDS Profile itself, then this list of values should be specified here.

hh.06-DE.07
"Data" means any data or information accessible via an Exchange by or on behalf of a Network or its registered users, including, without limitation, personally identifying information and protected health information.

ss.05-DE.07
"Health data" is written, electronic, oral, telephone, or visual information, identifiable or population based, that relates to an individual's or population's past, present or future physical or mental health status, condition, treatment, service or products purchased and includes, but is not limited to, laboratory test data or samples;

ph.09-DE.07
"Patient Data" means information provided by a Data Provider pursuant to Section 7.2 (Provision of Data).

ph.06-DE.07
Databases. Databases refers to the information and data collected by all providers participating in the [State Organization] Network.

pp.05-DE.07
III. The Immunization Data provided through from [Entity] is primarily derived from health care providers, including but not limited to Providers under contract with the Insurer, who make use of the Information System and have assumed contractual obligations to [Entity] to ensure that the Immunization Data in the database is true, accurate and complete, by entry into a Health Care Provider Information Sharing Agreement with [Entity]. The Insurer may therefore rely upon the Immunization Data received through [Entity] under this Agreement just as if it were provided from the clinical records maintained by Providers for its Enrollees.

mm.10-DE-07
"Health data" is written, electronic or visual information that relates to an individual's or population's past, present or future physical or mental health status, condition, treatment, service or products purchased and includes, but is not limited to, laboratory test data or samples.

mm.04-DE.07
Defining an Adequate Record

The record must be:

- A reliable basis for patient care.
- Confidential between physician and patient, and private as to third parties.
- Admissible as evidence in court.

mm.04-DE.07
A reliable basis for patient care is:

- Based on physician/nurse observation and patient presentation.
- Non-repudiable, accurate and complete.
- Available when needed.

mm.04-DE.07
A non-repudiable record is created by:

- Data sources bound by contract or policy
- Data from authenticated sources
- Careful classification of data
- A high integrity system platform

mm.09–DE.07
The Electronic Health Record (EHR) is an electronic record of a patient's health information generated by the patient's encounters in any care-delivery setting, from hospitalizations to visits with the family physician. Included in this record are patient demographics, progress notes, problems, medication history, vital signs, past medical history, immunizations, allergies, laboratory data and radiology reports. Ideally, the EHR automates and streamlines the clinician's workflow, allowing providers access to accurate, up-to-date patient information at the point of care. The EHR has the ability to generate a complete record of a clinical patient encounter while simultaneously providing secure access to the record by multiple providers caring for the same patient. Most importantly, the EHR is designed to reduce medical errors and generate time and cost efficiencies.

mm.06-DE.07
Protected Health Information (or "PHI") refers to any patient data, whether written or oral, that (1) is created or received by or for [State Organization] or Provider; (2) relates to the patient's health; and (3) either identifies the individual or for which there is a reasonable basis to believe could identify the patient.

mm.10-DE.07
XDS Affinity Domains can refine the use of many attributes of XDS Profile Transactions and attributes of the contents of the supported XDS Content Profiles. Frequently this involves restricting attributes to using certain defined sets of values, or mandating the manner in which the fields of an attribute's data type are used. In the case of Metadata attributes, their values are explicitly defined as being "XDS Affinity Domain specific" by the XDS Profile itself.

mm.10-DE.07
In addition, XDS Affinity Domains can refine the attributes of XDS Transactions or Content so they are required to be supported rather than optional as stated in the XDS Profile or the definition of the Content for the XDS Content Profile.

mm.10-DE.07
XDS Registry Metadata

Define all ways in which the XDS Affinity Domain refines Metadata attributes of an XDS Submission Set or an XDS Folder. It must specify any refinements to the way these attributes are used or to the sets of values that can be assigned to them. In addition, it may be useful for it to provide a translation to the language(s) of the XDS Affinity Domain of ITI TF-2: Table 3.14.4.1-6 Submission Set Metadata Attribute Definitions.

mm.10-DE.07
If a translation is not provided here then the following table should list all of the Submission Set Metadata Attributes from ITI TF-2: Table 3.14.4.1-6 whose use is refined in any way.

DE.08 Definition of Agreement

ph.09-DE.08
"Registration Agreement" means a legally binding agreement between the SNO and a Participant pursuant to which the SNO registers the Participant in accordance with, and the Participant agrees to comply with, the SNO Terms and Conditions.

ph.06-DE.08
"Registration Agreement" means a legally binding agreement between [SNO Name] and a Participant pursuant to which [SNO Name] registers the Participant in accordance with, and the Participant agrees to comply with, the Terms and Conditions.

ph.06-DE.08
4.2 Registration by Agreement. How Participants may enter into a written Registration Agreement with the SNO. A person may register with [SNO Name] as a Participant by entering into a written Registration Agreement with [SNO Name]. Such a Registration Agreement shall describe (a) the Participant's Participant Type, as described in Section 4.3.2 (Participant Type); (b) whether the Participant is a Data Provider or a Data Recipient, or both; (c) if the Participant is registered as a Data Recipient, which of the Services the Participant may use; and (d) such other terms and conditions as [SNO Name] and the Participant shall agree.

DE.09 Definition of Services

ph.06-DE.09
"Services" means the information-sharing and aggregation services and/or software described in Section 1.3 (Description of Services) for which the Participant registers as described in Section 4.1 (Registration Required).

ph.09-DE.09
"SNO's Services" means the information sharing and aggregation services and software described in Section 1.3 (Description of Services) for which the Participant registers as described in Section 4.1 (Registration Required).

ph.09-DE.09
1.3 Description of Services. The facilities and services of the SNO that are subject to the SNO Terms and Conditions, and that are available to Participants.

mm.09–DE.09
Health Information Exchange (HIE) is the term used to describe the secure exchange of a patient's medical information among approved providers, payers and patients. Ideally, multiple providers caring for the same patient would share and exchange relevant information, thus providing that patient with streamlined, more efficient care. Billing information would be transmitted electronically, thereby reducing paperwork and administrative costs. HIE allows the patient's record to be stored and accessed from multiple locations.

DE.10 Definition of Network

pp.06-DE.10
Section 1.11 Network. The term "Network" shall mean the [City] Regional Network for Primary and Emergency Care as described in this Agreement.

ph.09-DE.10
Background. A SNO is to operate as a health information data exchange organization (both regional and affinity) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information.

ph.06-DE.10
Background. A SNO is to operate as a health information data exchange organization (both regional and affinity-based) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information made up of a "network of networks."

ph.06-DE.10
"System" means [SNO Name]'s Internet-based authenticated peer-to-peer computer system and search engine for patient health, demographic, and related information that assists its users in locating, and facilitates the sharing and aggregation of, patient data held by multiple health care organizations with disparate health information computer applications, and which allows Authorized Users to authenticate and communicate securely over an untrusted network to provide access to and to maintain the integrity of Patient Data.

DE.11 Miscellaneous Definitions Provisions

ph.06-DE.11
"Terms and Conditions" means the terms and conditions set forth in this document, as amended, repealed, and/or replaced from time to time as described herein.

ph.06-DE.11
The Model uses the legal term "person" to describe both individuals and legal entities (e.g., corporations, limited liability companies, partnerships, etc.). The Model provides that each Participant's registration will record whether the Participant is a Data Provider, a Data Recipient or both and, if the Participant is a Data Recipient, whether the Participant will be permitted to use some or all of the SNO's Services.

pp.06-DE.11
Section 1.01 Agreement. The term "Agreement" shall mean this document, namely the [City] Regional Network for Primary and Emergency Care Second Participants' Agreement.

Section 1.02 Business Associate. The term "Business Associate" shall mean [Organization] when it, pursuant to this Agreement:

(a) On behalf of a Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity, performs, or assists in the performance of:

A function or activity involving the use or disclosure of PHI, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
Any other function or activity regulated by the Privacy Rule; or

(b) Provides, other than in the capacity of a member of the workforce of a Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR § 164.501), management, administrative, accreditation, or financial services to or for a Covered Entity, where the provision of the service involves the disclosure of PHI from such covered entity, or from another business associate of the Covered Entity to the Business Associate.

Section 1.03 Covered Entity. The term Covered Entity shall mean a Participant that is a health care provider who transmits any health information in electronic form in connection with a transaction covered 45 CFR Parts 160, 162, or 164.

Section 1.04 Designated Record Set. The term "Designated Record Set" shall mean a group of records maintained by or for a Covered Entity that is: (a) the medical records and billing records about Individuals maintained by or for a covered health care provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used in whole or in part, by or for a Covered Entity to make decisions about Individuals. For these purposes, the term "record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Co Section 1.13 Parties. The term "Parties" shall mean [Organization], Full Participants, and Storing Participants.

Section 1.14 Privacy Rule. The term "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164.

Section 1.15 Protected Health Information ("PHI"). The term "Protected Health Information" and the abbreviation "PHI" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the individually identifiable health information created or received by Business Associate from or on behalf of a Covered Entity.

Section 1.16 [Organization]. The term "[Organization]" shall mean the [Organization] Institute, Inc. and its employees and research scientists.

Section 1.17 Required By Law. The term "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

Section 1.18 Secretary. The term "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

Section 1.19 Storing Participants. The term "Storing Participants" shall mean those participating entities that will only submit and store Information on the Network. A Storing Participant shall not have access to the Information stored on the Network except for the Information actually submitted by that Storing Participant. Additional Storing Participants may be added under the procedures in Section 11.02.

Section 1.20 Treatment. The term "Treatment" shall have the definition assigned to it by the Privacy Rule at 45 CFR § 164.501, namely, the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.

Section 1.05 First Agreement. The term "First Agreement" shall mean the [City] Regional Network for Primary and Emergency Care Participants' Agreement which was executed by the parties in 1998.

Section 1.06 Full Participants. The term "Full Participants" shall mean those participating entities that will both submit and store Information on the Network and have access to the Network Information under the terms of this Agreement. The current Full Participants shall be: [Name] Health Partners, Community Hospital of [State] (and its affiliates and subsidiaries), [Name] Medical Group — Primary Care, [Name] Hospital and Health Centers, [Name] Hospital and Health Care Center, Inc., and [Name] Memorial Hospital. Additional Full Participants may be added under the procedures in Section 11.02.

Section 1.07 HHS. The term "HHS" shall mean the United States Department of Health and Human Services.

Section 1.08 Individual. The term "Individual" shall mean a person who is the subject of PHI, and shall have the same meaning as the term "individual" as defined in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

Section 1.09 Information. The term "Information" shall mean written or electronic patient information relating to a patient's diagnosis, treatment, tests, or prognosis stored by the Participants on the Network. Such Information may include, but not be limited to, admission, discharge, transfer, medical, prescription, billing, and/or other data for patients seen at, or provided laboratory services or prescription medication, at the Participants' facilities or offices.

Section 1.10 Limited Data Set. The term "Limited Data Set" shall mean PHI that excludes all direct identifiers of an Individual or of all relatives, employers, or household members of the Individual that are required to be removed pursuant to 45 CFR § 164.514(e).

mm.10-DE-11

A "deadly agent" is the causative agent of an illness or health condition sufficient to trigger the implementation of emergency response procedures or reporting requirements or requests under the governing law or regulations of any of the signatories' jurisdictions or of the Governments of the United States or Canada; or

an agent which, under the signatories' respective statutes or regulations, must be reported to or by the signatories' health agencies or ministries; or

an agent which, under the governing law or regulations of the Governments of the United States or Canada, must or is requested to be reported to the health agencies or ministries of the United States or Canada.

mm.10-DE-11

An "evacuee" means a person who by order, direction or request of a signatory, temporarily leaves his or her signatory jurisdiction of residence (the sending signatory) and removes to another signatory (the receiving signatory).

mm.10-DE-11
"[Name] U.S. Labs MOU" refers to the Memorandum of Understanding between the [State] Department of Health and Social Services, the [State] Department of Health and Welfare, the [State] Department of Human Services and the [State] State Department of Health of August 2004 and associated Attachments.

mm.10-DE-11
A "public health emergency" is an occurrence or imminent threat of an illness or health condition sufficient to trigger the implementation of emergency health response procedures or reporting requirements or requests under the governing law or regulations of any of the signatories' jurisdictions or of the Governments of the United States or Canada.

mm.10-DE-11
A "refugee" means a person who by order, direction or request of his signatory jurisdiction of residence (the sending signatory), temporarily refrains from returning to his jurisdiction of residence and remains within another signatory jurisdiction (the receiving signatory).

ph.02-DE.11
A. RESEARCHER is ___________________________ a syndromal surveillance system for public health purposes, named "REDACTED" ("BIOSURVEILLANCE"). BIOSURVEILLANCE is intended to provide for REDACTED and other events affecting public health, by obtaining and analyzing REDACTED data from multiple hospitals through online reporting of specified data on a regional basis. In order to further the development of BIOSURVEILLANCE, REDACTED.

ph.02-DE.11
B. PROVIDER/REPOSITORY is a provider of REDACTED, including REDACTED clinical data in electronic form on behalf of a number of hospitals. Some of the clinical data hosted by PROVIDER/REPOSITORY includes clinical data sets suitable for use in research testing BIOSURVEILLANCE.

ph.02-DE.11
C. Data Provider is a hospital which has contracted with PROVIDER/REPOSITORY for REDACTED services including the hosting of electronic clinical data. Some of this data is suitable for use in REDACTED BIOSURVEILLANCE.

ph.02-DE.11
D. RESEARCHER, PROVIDER/REPOSITORY and Data Provider wish to make electronic clinical data owned by the Data Provider and hosted by PROVIDER/REPOSITORY available for research in BIOSURVEILLANCE, subject to assurances that such data will not be used or disclosed for any other purpose, and will be protected against any use or disclosure not expressly authorized by this Agreement.

The parties therefore agree:

mm.09-DE.11
The Electronic Health Record (EHR) is an electronic record of a patient's health information generated by the patient's encounters in any care-delivery setting, from hospitalizations to visits with the family physician. Included in this record are patient demographics, progress notes, problems, medication history, vital signs, past medical history, immunizations, allergies, laboratory data and radiology reports. Ideally, the EHR automates and streamlines the clinician's workflow, allowing providers access to accurate, up-to-date patient information at the point of care. The EHR has the ability to generate a complete record of a

clinical patient encounter while simultaneously providing secure access to the record by multiple providers caring for the same patient. Most importantly, the EHR is designed to reduce medical errors and generate time and cost efficiencies.

mm.09-DE.11
The Personal Health Record (PHR) is another important component of the Electronic Health Record. The PHR is an Internet-based tool that allows patients to access and coordinate their lifelong health information, make appropriate parts of it available to those who need it, and gives the patient an ownership role in managing his or her medical record.

mm.09-DE.11
Health Information Exchange (HIE) is the term used to describe the secure exchange of a patient's medical information among approved providers, payers and patients. Ideally, multiple providers caring for the same patient would share and exchange relevant information, thus providing that patient with streamlined, more efficient care. Billing information would be transmitted electronically, thereby reducing paperwork and administrative costs. HIE allows the patient's record to be stored and accessed from multiple locations.

ph.06-DE.11
Protected Health Information. Protected Health Information (PHI) shall have the same meaning as the terms "Protected Health Information" or "PHI" in the Privacy Rule.

ph.06-DE.11
Required by Law. Required by Law shall have the same meaning as the term Required by Law in the Privacy Rule.

mm.06-DE.11
Disclosure means the release or transfer of PHI outside [State Organization] or Provider, or permitting access to PHI from outside [State Organization] or Provider.

mm.06-DE.11
Protected Health Information (or "PHI") refers to any patient data, whether written or oral, that (1) is created or received by or for [State Organization] or Provider; (2) relates to the patient's health; and (3) either identifies the individual or for which there is a reasonable basis to believe could identify the patient.

mm.06-DE.11
Use means sharing, accessing, examining, applying, or analyzing PHI within [State Organization].

ph.09-DE.11
Defined Terms. The Model assumes that a variety of different types of entities will participate in the SNO, and that these Participants will have a variety of roles. Section 2 (Definitions) of the Model provides a framework for naming these different Participants and their respective roles.

For each section of the Model, this document provides a brief description of the contents of the section and the critical legal and policy issues raised by each. For some sections, alternative provisions are offered.

Model Terms and Conditions
Topic List

1. Introduction. A description of the Sub-Network Organization or "SNO" and how it is organized and operated, to provide information that may be helpful for putting the remainder of the Terms and Conditions into context.

ph.09-DE.11
"SNO Terms and Conditions" means the terms and conditions set forth in this document, as amended, repealed and/or replaced from time to time as described herein.

ph.06-DE.11
Defined Terms. The Model assumes that a variety of different types of entities will participate in the SNO, and that these Participants will have a variety of roles. Section 2 (Definitions) of the Model provides a framework for naming these different Participants and their respective roles. For each section of the Model, this document provides a brief description of the contents of the section and the critical legal and policy issues raised by each. For some sections, alternative provisions are offered.

ph.06-DE11
The Model uses the legal term "license" to describe the specific rights to be granted to each Data Recipient.

ph.06-DE.11
The Model uses the legal term "license" to describe the specific rights to be granted to each Data Provider. The Model generally restricts the Data Provider's rights to access the SNO's System to those necessary to provide data in accordance with Section 7.2 (Provision of Data).

ss.05-DE.11
An "infectious disease agent" is the causative agent of an illness or health condition that may trigger reporting requirements or requests under the governing law or regulations of any of the signatories' jurisdictions or of the Governments of the United States or Canada or implementation of public health protection measures and/or emergency response procedures;

ss.05-DE.11
A "public health event" is an occurrence or imminent threat of an illness, communicable disease or health condition with the potential for cross-border implications that could trigger implementation of emergency health response procedures or reporting requirements or requests wader the governing law or regulations of any of the signatories' jurisdictions or of the Governments of the United States or Canada.

sp.02-DE.11
(vi) HHS means the United States Department of Health and Human Services.

sp.02-DE.11
(iii) Data Subject means a natural person who is the subject of Protected Information, including but not limited to an "individual" under 45 CFR § 164.501.

mm.10-DE.11 Glossary
Glossary of terms specific to the XDS Affinity Domain extension.

mm.10-DE.11
Terminology and Content
Introduction

If the IHE XDS Profile or XDS Content Profiles are refined in any way then describe this here. Typically the following types of refinements are made:

mm.10-DE.11
Such refinements must not break conformance with the XDS Profile or to the defined Content of the XDS Content Profiles being supported. For example, it is not acceptable to lower the requirement of an attribute to be optional when it is defined to be required for XDS Metadata or Content.

mm.10-DE.11
This introductory section explains any principle areas of terminology and content that are refined by the XDS Affinity Domain. In addition, if there is any overall philosophy followed in defining these then this should also be explained here.

mm.10-DE.11
For example if there is some overall way in which any object identifier value (i.e. for patient IDs, practitioner ID, etc.) must be created then this should be specified as part of the introduction to this terminology section.

mm.10-DE.11
Common Rules for Identifier Construction (example)

This terminology sub-section serves as an example of where general rules for constructing any identifier for this XDS Affinity Domain should be specified. For example, this sub-section could specify rules for creating OIDs to be used in this XDS Affinity Domain.

mm.10-DE.11
Submission Set Metadata

If the language used in the XDS Affinity Domain is not English and a translation of the entire IHE ITI Technical Framework has not been done then this section should provide a translation of the ITI TF-2: Table 3.14.4.1-6 Submission Set Metadata Attribute Definitions, to one of the languages. If more than one language exists in the XDS Affinity Domain then this entire section and its sub-sections should be repeated for each of these languages.

mm.10-DE.11
Submission Set Metadata Attribute Definitions

XDS Document Entry Attribute

Refinement of Attribute

Source/Query
(Bold and Underline if refined)

Data Type

Author Institution

Provide a translation if necessary.

Define whether or not the XDS Affinity Domain refines the use of this Attribute in any way. If not then it is not mandatory to list the attribute here. Otherwise, point to the sub-section of ______ that explains the refinement of this Attribute for the extension. If the Attribute is refined by defining a Source or Query value that is different from the Technical Framework (i.e. by requiring a value whereas it is optional in the Framework) then bold and underline the altered value and provide an explanation in the sub-section. Same applies for the remaining Attributes.

R2/R

Provide a reference to the sub-section of ______ that specifies the list of permitted XON data type author Institution values for the of this attribute.

For this example, "Refer to ______ for the XDS Affinity Domain specification of this Attribute".

etc…

Create a sub-section for each Submission Set Metadata Attribute that is refined for the XDS Affinity Domain.

mm.10-DE.11
Refinement of author Institution (example)

This sub-section for the author Institution Metadata Attribute should state how the values for this attribute are specified for this XDS Affinity Domain.

mm.10-DE.11
For example, author Institution, has an HL7 Data Type of XON so the author Institution sub-section could specify the sets of permitted values for each field of the XON Data Type for author Institution.

mm.10-DE.11 HL7 V2.5 Component Table - XON – for author Institution
Specification of Organization Name component (example)

This sub-section for the author Institution Metadata Attribute should state how the Organization Name component is specified for this XDS Affinity Domain.

mm.10-DE.11
Etc.

Sub-section for specification of each remaining XON Data Type component for author Institution.

mm.10-DE.11
Folder Metadata

If the language used in the XDS Affinity Domain is not English and a translation of the entire IHE ITI Technical Framework has not been done then this section should provide a translation of the ITI TF-2: Table 3.14.4.1-7 Folder Metadata Attribute Definitions, to one of the languages. If more than one language exists in the XDS Affinity Domain then this entire section and its sub-sections should be repeated for each of these languages.

mm.10-DE.11
If a translation is not provided here then the following table should list all of the Folder Metadata Attributes from ITI TF-2: Table 3.14.4.1-7 whose use is refined in any way for this XDS Affinity Domain.

mm.10-DE.11
In either case, there should be a comment for each listed attribute indicating if the use of the attribute is refined in any way for the XDS Affinity Domain. If so then the comments must indicate how this is done. Unless this can be explained very briefly then it should provide a link to a following sub-section that includes text describing how the attribute's use is refined. For example, this could require defining the set of possible values that can be used for the attribute.

Folder Metadata Attribute Definitions

Create a sub-section for each Folder Metadata Attribute that is refined for the XDS Affinity Domain.

mm.10-DE.11
Refinement of code List (example)
This sub-section for the code List Folder Metadata Attribute should state how the values for this attribute are specified for this XDS Affinity Domain.

mm.10-DE.11
For example, the code List sub-section could specify the set of permitted values (Code Value, Display Name, and Coding Scheme Designator).

mm.09-DE.11
To identify those cases of infectious diseases which are of interest to both countries, this document uses the term "binational case" to refer to an individual with a confirmed or probable case of a notifiable infectious disease, and:

- who has recently traveled or lived in the neighboring country, or had recent contact with persons who lived or traveled in the neighboring country; or
- who is thought to have acquired the infection in the neighboring country or have been in the neighboring country during the incubation period of the infection and was possibly contagious during this period; or
- who is thought to have acquired the infection from a product from the other country; or
- whose case requires the collaboration of both countries for the purposes of disease investigation and control.

mm.09-DE.11
5. Specific Guidelines

This section presents specific guidelines for different types of events and for different areas of collaboration.

5.1 Binational Cases

As stated earlier, a binational case refers to an individual with a confirmed or probable case of a notifiable infectious disease who may have acquired or may transmit the disease in the other country, or who may require binational collaboration for investigation and/or control. An example of a binational case is a person with tuberculosis under treatment who crosses the border during the course of his or her medical care and public health follow-up. Such a binational TB case is thus at risk for interruptions in treatment with the consequent possibility of transmitting TB to others, as well as of developing drug resistant tuberculosis.

Based on the "Need to Share Information" (General Principle 2.1) identification of binational cases by public health authorities warrants the sharing of relevant information with counterparts of the neighboring country to assist in finding other cases, to limit the risks of further disease transmission, and to ensure adequate control of the disease among identified cases.

mm.09-DE.11
5.2 Binational Outbreaks

The term outbreak is considered to represent a significant increase over the expected number of cases of a specific notifiable disease or other health problem in a given population over a given time period. The number of cases required to consider a cluster of disease cases an outbreak thus obviously depends on historical epidemiologic data and diagnostic criteria and laboratory resources. A single case of a rare disease, such as rabies or an "eradicated" disease such as smallpox, may constitute an outbreak, while numerous cases of more common diseases such as HIV/AIDS or tuberculosis may be required to be considered an outbreak. Newer diagnostic capabilities such as molecular fingerprinting techniques can identify a cluster of illnesses with indistinguishable molecular fingerprints; epidemiological investigation is then used to find links between these illnesses in the cluster. This combination of molecular fingerprinting and epidemiological investigation has identified numerous outbreaks, including widely dispersed outbreaks that would otherwise have gone undetected. An outbreak is considered binational:

- when disease exposures occur in one country to visitors or migrants of the other country,
- when disease is associated with products from the other country, or
- when cases appear in border settings involving the population from both countries.

sp.08-DE.11
View Immunizations means the user has permission to view the entire immunization history and status (i.e., whether or not the child is up-to-date with recommended immunizations).

sp.08-DE.11
View Demographics means the user can view information about the child, including the child's name, date of birth, parent/guardian name, address and telephone number.

sp.08-DE.11
Add/Edit Information means the user can add new immunizations to a child's record and edit immunizations already previously recorded in a child's record. Providers may add a new child record into the [Immunization] Registry database or alter the details on a child already contained in the [Immunization] Registry database.

ph.06-DE.11
Definitions. "Documentation" means the user documentation, manuals, and user guides, whether in paper, electronic, or other form, furnished to Hospital by Network for use with the Exchange.

mm.06-DE.11
Mission. The Exchange's mission is to enhance patient safety and the efficient provision of quality patient care in _____________________.

Goals. The Exchange will enhance patient care by:

- Speeding health care providers' access to critical patient information.
- Providing a longitudinal view of the patient's medical history across Exchange health care providers.
- Reducing health care costs through automation and reducing duplicative tests.
- Reducing medical errors created by incomplete or incorrect information in patient medical records.

Governing Body. The governing body of Exchange is the Board of Directors of the ___________________ ("Network").

4.2 Recitals (RE)

RE.01 Description of HIE

ph.06-RE.01
Background. A SNO is to operate as a health information data exchange organization (both regional and affinity-based) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information made up of a "network of networks."

sp.08-RE.01
Pursuant to its public health authority under section 6-210 of the [City] Health Code which mandates reporting of immunization data for persons 0-18 years of age and the creation and maintenance of a citywide immunization registry, the [City] Department of Public Health (City DPH), Immunization Program has created the Immunization Database/Tracking System ([Immunization]), heretofore referred to as the [Immunization] Registry.

sp.08-RE.01
In order to increase appropriate immunizations among preschool children, every child residing in [City] is enrolled in the Registry, using information derived from the [State] Bureau of Vital Statistics.

ph.06-RE.01
WHEREAS, Network has established a secure, electronic patient data exchange system to allow authorized users to electronically access patient information from participating health care providers ("Exchange"); and

hh.06-RE.01
WHEREAS, Networks have established secure, electronic patient data exchange systems (the "Exchanges") to allow Authorized Users (as defined below) to electronically access patient information from other Authorized Users; and

hh.06-RE.01
WHEREAS, Networks have entered into agreements with health care entities under which each Authorized User has agreed to provide the Networks' designated "Registered Users" with access to an Exchange in order to view patient information generated by participating Authorized Users; and

ph.06-RE.01
SNO Organization and Operations. The Model assumes that the SNO is a nonprofit or for-profit legal entity that is organized and operated for a single purpose, i.e., to operate as a SNO. The SNO is assumed to operate with a record locator service-based, peer-to-peer

network, and to provide, or provide access to, the software Participants require to use the SNO's Services. SNOs may provide a different system or services, such as by acting as an application service provider ("ASP"), and the Model identifies some of the variations that are likely if the SNO is organized differently from what the Model assumes.

ss.05-RE.01
Nothing in this Agreement precludes additional jurisdictions with public health responsibilities in the [Region] from becoming signatories, subject to approval of the working group,

sp.02-RE.01
A. The Clinical Outcomes Assessment Program ("[Program]") is a program facilitated by the Foundation for Health Care Quality ("[Entity]") which collects and analyzes cardiac care clinical outcomes information from and on behalf of health care providers. This data is collected, maintained, processed and distributed in electronic form through an information system including database(s) which constitute a cardiac registry system ("[Program] Cardiac Registry").

ph.06-RE.01
1. Introduction. A description of the sub-network organization or ("SNO") and how it is organized and operated, in order to provide information that may be helpful for putting the remainder of the Terms and Conditions into context. The SNO may choose to omit some or all of this section if it is found to be unnecessary.

ph.09-RE.01
SNO Organization and Operations. The Model assumes that the SNO is a non-profit or for-profit legal entity that is organized and operated for a single purpose, i.e., to operate as a SNO. The SNO is assumed to operate with a record locator service-based, peer to peer network, and to provide, or provide access to, the software Participants require to use the SNO's Services. SNOs may provide a different system or services, such as by acting as an application service provider ("ASP"), and the Model identifies some of the variations that are likely if the SNO is organized differently from what the Model assumes.

ph.09-RE.01
Background. A SNO is to operate as a health information data exchange organization (both regional and affinity) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information.

ph.06-RE.01
WHEREAS, [State Organization] is a health information exchange (HIE) organization formed for the purpose of facilitating HIE between and among providers, patients and authorized third-party entities. As part of this activity, [State Organization] allows participating providers who enter into and comply with this Agreement access to personal health information held by other participating organizations through the [State Organization] Network (the "Network").

ph.06-RE.01
Whereas, [RHIO] is a [State] nonprofit corporation organized for one or more purposes recognized as exempt from federal income taxation, including the improvement of the quality, safety and efficiency of the delivery of healthcare through enabling the electronically interoperable delivery of clinical data to the point of care.

ph.09-RE.01
Background. A SNO is to operate as a health information data exchange organization (both regional and affinity) that operates as a part of the National Health Information Network ("NHIN"), a nationwide environment for the electronic exchange of health information.

RE.02 Description of non-HIE Party

ph.05-RE.02
NOW, THEREFORE, the parties, in consideration of the mutual promises and obligations set forth herein, the sufficiency of which is hereby acknowledged, and intending to be legally bound, agree as follows:

The following individuals (the "Authorized Parties") are authorized to use the Limited Data Set or any part of it on behalf of User and agree to abide by the terms of this Agreement:
Name: ____ Signature: ____
Name: ____ Signature: ____

Use an attachment to list any additional individuals. The attachment must be signed by authorized representatives of User and The Regents.

hh.06-RE.02
Each Network may enroll the following types of entities as Authorized Users:

- Hospitals, physicians;
- Payors
- Clearinghouses; and
- Other health care providers subject to HIPAA.

Introduction

The concept of an XDS Affinity Domain is defined in ITI TF-1:10 and Appendix K. It is clear that many regulatory/professional organizations will need to define policies regarding coded terminology, privacy, document format and content, language support, etc. for an XDS Affinity Domain. In addition, there will be the need to define such policies on a national or regional basis for all XDS Affinity Domains within a geographic region. These policy decisions, necessary for successful implementation, may result in refinements of the XDS Profile itself.

sp.02-RE.02
10. Participant Information.

(Please type or print all information)
By executing below, the Participant accepts the terms and conditions of this agreement:

Name of Participant:
Contact Person and Title:
Mailing Address:
City/State/Zip:
Phone: Fax: E-mail:

Physicians (Names & Titles) Authorized to Access Information on Behalf of Participant:
Use additional sheet if necessary.

Full Name Title

1. ________________________________ ________________________________

2. ________________________________ ________________________________

3. ________________________________ ________________________________

4. ________________________________ ________________________________

5. ________________________________ ________________________________

6. ________________________________ ________________________________

pp.05-RE.02
II. The Entity provides health care services by and through its individual Providers, including immunization services. The Providers wish to have the benefit of access to the Information Services provided by [Entity] to assist them in the provision of health care, and the Entity wishes to allow for such access.

pp.05-RE.02
I. The Health Information Institute, Inc. is a [State] corporation ("[Entity]") which serves as a communications link, data repository and data retrieval facility for health care providers, to permit them to share information about the immunization status of children and adults in their care with other providers. [Entity] maintains a health care information system and immunization history database which is directly linked to health care providers' offices, and may be linked into their computer-based patient information systems.

pp.05-RE.02
II. The Provider who is entering into this Agreement is (check one):

An individual who is licensed, certified, registered or otherwise authorized by the laws of the State of [State] to provide health care in the practice of his or her profession or the ordinary course of his or her business.

pp.05-RE.02
A professional corporation or limited liability company, public agency or other entity or organization which is authorized or otherwise qualified to and does provide health care services through individual shareholders, members, officers, employees, contractors, or other personnel who are licensed, certified, registered or otherwise authorized to provide health care in the practice of their profession(s) or the ordinary course of their business(es).

pp.05-RE.02
1) The Health Information Institute, Inc. is a [State] corporation ("[Entity]") which serves as a communications link, data repository and data retrieval facility for health care providers, to permit them to share information about the immunization status of children and adults in their care with other providers. [Entity] maintains a health care information system and immunization history database which is directly linked to health care providers' offices, and may be linked into their computer-based patient information systems.

pp.05-RE.02
1) The Provider who is entering into this Agreement is an individual who is licensed, certified, registered or otherwise authorized by the laws of the State of [State] to provide health care in the practice of his or her profession or the ordinary course of his or her

business. The obligations of this Agreement shall bind not only the Provider but the Provider's staff, employees or agents who are authorized to act on behalf of the Provider in obtaining and/or making records of health care information about persons who receive health care from the Provider.

pp.05-RE.02
1) This Agreement is for the benefit and use of the Provider as an individual health care provider only. If the Provider provides health care as a partner, officer, member, employee or other agent or participant in a partnership, corporation, limited liability company, or other private enterprise or government agency, [Entity] may contract directly with such enterprise or agency to assume financial responsibility for the Provider's payment obligations under this Agreement. No such contract shall relieve the Provider of its other obligations under this Agreement.

pp.05-RE.02
I. The Health Information Institute, Inc. ("[Entity]") is a [State] corporation which serves as a communications link, data repository and data retrieval facility for health care providers, to permit them to share information about the immunization status of children and adults in their care with other providers ("Immunization Data"). [Entity] maintains a health care information system and immunization history database (hereafter known as "Information System") which is directly linked to health care providers' offices, and may be linked into their computer-based patient information systems.

pp.05-RE.02
II. _______________ ("Insurer") is an insurance company authorized by the Office of the Insurance Commissioner of the State of [State] to provide health insurance benefits to individuals in the state of [State] ("Enrollees"), for health care services provided by entities and persons under contract with the Insurer who are licensed, certified, registered or otherwise authorized to provide such services to individuals in the practice of their profession(s) or the ordinary course of their business(es)("Providers").

ph.06-RE.02
Whereas, Participant is a [State] nonprofit corporation which owns and operates a pediatric hospital in the state of [State];

sp.02-RE.02
B. [Entity] maintains and operates the [Program] Cardiac Registry to provide information for purposes of planning, quality assessment and improvement and other related functions, by health care providers participating in [Program] ("Participants"), and for purposes of research under appropriate conditions.

sp.02-RE.02
Health care providers which agree to be bound by these policies and procedures and enter into an agreement in the form of the present Agreement are entitled to participate in [Program].

sp.02-RE.02
C. The undersigned health care provider (hereafter "Participant") wishes to participate in [Program] and enter into this Agreement. The Participant is (check one):

[ ] A health care provider who is already a Participant in the [Program] program, and wishes to enter into this Agreement to amend and restate the Participant's existing agreement.

[ ] An individual who is not already a Participant in the [Program] Program, who is licensed, certified, registered or otherwise authorized to provide health care in the practice of his or her profession or in the ordinary course of his or her business, in the state(s) in which he or she provides such services (hereafter "Individual Provider").

[ ] A professional corporation, institution or limited liability company, public agency or other entity or organization which is not already a Participant in the [Program] Program, and is authorized or otherwise legally qualified to and does provide health care services through individual shareholders, members, officers, employees, contractors, or other personnel who are licensed, certified, registered or otherwise authorized to provide health care in the practice of their profession(s) or the ordinary course of business(es) (hereafter "Institutional Provider").

If the undersigned Participant is an Institutional Provider, it hereby acknowledges that it is entering into this Agreement for and on behalf of both itself and for the Individual Providers associated with it.

RE.03 Statement of Purposes of the Agreement

ss.05-RE.03
The signatories recognize the, importance of safeguarding individuals' privacy in exchanging and using health data while simultaneously recognizing a compelling interest on the part of the signatories to share health data to prevent, detect and respond to public health events for the protection of public health and safety.

ss.08-RE.03
WHEREAS the delivery of health care can occur in many different settings, sometimes crossing geographical boundaries; and

ss.08-RE.03
WHEREAS there is a need to transmit health care data to health care providers in a clinically useful form regardless of setting or location; and

ss.08-RE.03
WHEREAS there has been limited exchange of such health care data between states; and

ss.08-RE.03
WHEREAS the purpose of this Agreement is to provide for health data sharing by specifying the deliverables required of this pilot test for the sharing/exchange of immunization data between the following electronic applications: the [State] Immunization Information System, the [City] Immunization Registry, and/or the [State] State Immunization Information System; and

ss.08-RE.03
WHEREAS the scope of this pilot will include sharing/exchanging vaccination data, patient name, date of birth, demographic information, the location at which the vaccination was administered, the vaccine received, the date of administration, the medical professional who provided the service and the patients' insurance information, whether they are VFC eligible, privately insured or Medicaid; and

ss.08-RE.03
WHEREAS the immunization data will be extracted from the [City] DOH and transmitted to the [State] DOH for transmission to the [State] IIS system; and immunization data will be

extracted from the [State] IIS in an agreed upon format and sent to the [State] DOH for transmission to the [City]; and

ss.08-RE.03
WHEREAS information for individuals whose place of residence is in [State] but that receive immunization vaccinations in [State] or [City] and data regarding [City] and [State] residents who do not have a [State] address but receive immunization care in [State] will be shared and exchanged; and

ss.08-RE.03
WHEREAS this pilot test is a preliminary step to developing an architectural framework between the [State Department] and the [City] DOH and/or the [State] DOH for standardized naming conventions, data storage, communication processes, integrity, security, and data privacy that will improve public health functions, integration and evaluation, research and better access to health data leading to improved patient care; and

ss.08-RE.03
WHEREAS the [State Department]has the statutory authority under [Statute], et seq., the Statewide Immunization Registry Act, specifically at [Statute] to share and obtain immunization data on [State] residents from sources that house that information stating,: 'The provisions of this act shall not prohibit the transmission or exchange of information from other government database systems, immunization registries of other states or similar regional registries officially recognized by those states, health maintenance organizations or health benefits plans, health insurance companies, practice management or billing vendors, or other similar databases containing immunization histories, if the transmission is in accordance with the provisions of this act and other relevant State and federal laws and regulations." under Public Health Law S.A. (Insert PLA Here); and

ss.08-RE.03
WHEREAS the [State Department] finds it in the public interest to participate in this collaborative pilot test as a preliminary step to improving provider access to timely health data for the provision of better health care for each state's patient population; and

ss.08-RE.03
WHEREAS the DOH [Insert the name of the other State Agency.]has the statutory authority under Public Health Law Section [#] that provides that "the Commissioner may provide registrant specific immunization records to other state registries pursuant to written agreement requiring that the foreign registry conform to national standards for maintaining the integrity of the data and will not be used for purposes inconsistent with the provisions of this section." The section allows for the sharing/exchange of immunization health information data with the [State Department]/[Department] through the Departments' Office of [Department] provision for the technical expertise of the Project Manager assigned to the IIS Registry to prepare the data files and transmit the immunization information to the [State] DOH for [City] DOH, and

WHEREAS Public Health Law Section [#] requires that the [City] provide immunization information to the [State] DOH Commissioner.

ss.08-RE.03
AND WHEREAS the [State] DOH and the [City] DOH finds it necessary to enter into an agreement with the [State Department] that will allow the pilot test to occur; and

ss.08-RE.03
WHEREAS the [City] DOH finds it in the public interest to participate in this collaborative pilot test as the initial step toward improving provider access to timely health data for the provision of better health care for each state's patient population; and

hh.06-RE.03
WHEREAS, Networks desire to participate in each other's Exchange in order to allow Authorized Users to contribute and access patient information for the continuing care and treatment of patients and beneficiaries; and

WHEREAS, each Network desires the other to have the same privileges to the Exchange as a "Registered User" has pursuant to the agreement between an Authorized User and a Network; and

sp.08-RE.03
Incorporation of Specifications Agreements. This Agreement incorporates by reference any Specifications Addendum which any two or more parties to this Agreement have agreed shall incorporate this Agreement by reference. Any such Specifications Addendum must include the provisions set forth in Section B(2) below.

Intent to Comply with Laws. This Agreement shall be interpreted consistently with all applicable Information Privacy and Protection Laws, and shall be construed and interpreted liberally in favor of the protection of Protected and confidential Information. In the event of a conflict between applicable laws, the more stringent law shall be applied.

mm.06-RE.03
In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties therefore agree as follows:

Interpretation of this Agreement.

Definitions. All DE.11 except those specifically marked

Capitalized terms in this Agreement are defined in the text or as follows:

"Access" means the ability, means or act of reading, writing, modifying or otherwise communicating data or information or making use of any computer system resource.[3]

"Aggregate" means to combine information from a Disclosing Party with information Received from another source.[4]

"Security" means that set of policies, processes and procedures adopted by a party to ensure the Protection of Information.[5]

"Specifications Addendum" means an addendum to this Agreement which defines the specifications and procedures for Disclosure of information by a party to this Agreement. In the event that more than one party is Disclosing information to another party to this Agreement, the parties may agree to establish Specifications Addenda for each party. Each Specifications Addendum shall be identified by the name of the Disclosing Party to which it applies. All Specifications Addenda shall be incorporated into this Agreement by reference.

[3] Draft Security Rule at 43,265, 45 CFR sec.142.304 (definition of "access").
[4] See Privacy Rule at 82,803, 45 CFR sec. 164.501 (definition of "data aggregation").
[5] Draft Security Rule at 43,249-250.

Specifications Addenda may be amended by the parties from time to time as provided below.

"Subcontractor" means a Third Party providing services to a Receiving Party in connection with the Receiving Party's obligations under this Agreement.[6]

"Term" means the period of time from the Effective Date through Termination of this Agreement.

"Third Party" means any individual, person or organization which is not a party to this Agreement.

"Transaction" means the Transmission of information between parties to this Agreement.[7]

"Transmit," "Transmitted" or "Transmission" means the transfer of information by one party to another, including (i) telephone voice and "faxback" systems, (ii) the transfer by mail or courier of information stored in portable electronic media or printed on paper or other "hard copy" medium, and (iii) electronic transmission by a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, and private networks.[8]

"Unauthorized" means (i) an individual or entity who has not been Authorized to act on behalf of a party, or (ii) an action by an Authorized individual or entity which is not within the scope of the Authorization.

"Use" means the sharing, employment, application, utilization, examination, analysis, anonymization, or commingling with other information, of information by a party which holds that information.[9]

"Workforce" means an party's employees, volunteers, trainees, and other persons under direct control of the party, including persons providing labor on an unpaid basis.[10]

"Writing" or "Written" means text created or recorded on paper or created or recorded in an electronic medium; provided that a copy of any electronic Writing must be recorded and archived in a trustworthy system of records in which its integrity and usability will be maintained and from which non-repudiable copies will be readily available for a period of no less than six (6) years from the date the copy is deposited.[11]

Application of Provisions to Multiple Parties. Any party to this Agreement may either Disclose Protected Information and other information to or Receive Protected Information and other information from any other party to this Agreement. The provisions applicable to a party will vary depending on whether the party is a Receiving Party or a Disclosing Party in any given Transaction.

[6] See Privacy Rule at 82,808 45 CFR sec. 164.504(e)(2)((ii)(D).

[7] See Privacy Rule at 82,800, 45 CFR sec. 160.103 (definition of "transaction").

[8] See Transactions Rule at 50,367, 45 CFR sec. 162.103 (definition of "electronic media").

[9] See Privacy Rule at 82,805, 45 CFR sec. 164.501 (definition of "use")

[10] See Privacy Regulations at 82,800, 45 CFR sec. 164.103 (definition of "workforce")

[11] See Privacy Rule at 82,828, 45 CFR sec. 164.530(j)(requiring that a Covered Entity must retain Electronic Records of its required privacy policies and procedures for at least six (6) years from the later of the date of its creation or the date it was last effective). See generally *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* (National Archives and Records Administration, October 18, 2000). The actual records retention period should probably be tied to the expected Term of the Agreement, plus the statute of limitations applicable to written contract actions under applicable state law.

mm.03-RE.03
Vision. The Exchange's vision is to develop and maintain an electronic health information system that provides a longitudinal electronic medical record for _________________ patients that can be accessed and updated in real time by authorized health care providers.

ph.06-RE.03
WHEREAS, Hospital desires to participate in the Exchange in order to contribute and access patient information for the continuing care and treatment of its patients; and

ph.06-RE.03
WHEREAS, Network desires Hospital to have the same privileges to the Exchange as a "Registered User" has pursuant to the End User Agreement between Access Provider and Network; and

ph.06-RE.03
WHEREAS, Network has entered into an agreement with ____________________ ("Access Provider") under which Access Provider has agreed to provide Network's designated "registered users" with access to the Exchange in order to view patient information generated by participating _ health care providers ("Data Providers"); and

WHEREAS, Network has entered into an agreement with __________________ ("Host") to host the Exchange; and

ph.05-RE.03
WHEREAS, The Regents maintains certain information that User wishes to use and/or disclose for research, public health, or health care operations purposes permitted under 45 C.F.R. § 164.514(e):

sp.02-RE.03
B. [Entity] maintains and operates the [Program] Cardiac Registry to provide information for purposes of planning, quality assessment and improvement and other related functions, by health care providers participating in [Program] ("Participants"), and for purposes of research under appropriate conditions.

mm.09-RE.03
The [Organization] Data Sharing Plan presents information about the data that the adopting institution will share via the [Network], including how, with whom, and when the data will be shared. The plan establishes the nature of the data for purposes of determining the sensitivity of the data (related to legal and ethical restrictions on data exchange, intellectual property value, and contractual obligations) and thus the access controls necessary to secure the data. The data sharing plan also presents information about the institution's internal approval processes for sharing data outside of the institution. That information is used to deepen the understanding of the broader [Organization] community about data sharing practices in general and to assist the individual adoption project and researcher in securing approval to share data.

mm.09-RE.03
The following list of topics to address is intended as a guideline or checklist to assist the researcher in preparing a Data Sharing Plan for use in a [Organization] adoption project.

ss.05-RE.03
The purpose of this Agreement is to facilitate sharing of public health related data, both individually identified and population-related, between signatories for the purpose, and no

additional purpose, of preventing, detecting or responding to a public health event, thus assuring prompt and effective identification of infectious disease and other agents that could affect public health in the [Region], and to prevent further spread of disease.

ph.06-RE.03
1.2 Purposes. The purposes for which the SNO is organized. [SNO Name] is organized to facilitate health information sharing and aggregation for treatment, payment, operations, public health and research-related purposes through the NHIN and in a manner that complies with all applicable laws and regulations, including without limitation those protecting the privacy and security of health information.

sp.06-RE.03
This agreement is needed as part of the review of your data request to ensure compliance to the requirements of the Privacy Act, and must be completed prior to the release of specified data files containing individual identifiers.

ph.06-RE.03
WHEREAS, Provider desires to obtain access to use the Network and, accordingly, has completed and executed the necessary portions of this Agreement, as well as reviewing and agreeing to the various policies of the Network.

ph.06-RE.03
WHEREAS, Although [State Organization] is not a Covered Entity under HIPAA, this Agreement is entered into for the purpose of protecting the confidentiality and security of patient information transmitted or communicated to Provider as part of or in connection to the Network and for complying with Provider's obligations under the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, 45 C.F.R. Parts 160 and 164 ("HIPAA").

mm.06-RE.03
The purpose of this policy is to ensure [Organization] and [Organization] participants that this entity will undertake disciplinary action against any person who violates the Provider's security policies and procedures and/or causes the Provider to violate the Provider Participation Agreement with [Organization].

mm.06-RE.03
The purpose of this Policy is to ensure that Provider personnel implement Provider's safeguards regarding the protection and privacy of Protected Health Information in utilizing [Organization].

ph.09-RE.03
Topic List Introduction. This document (Topic List) describes the issues addressed by the Connecting for Health Model Contract for Health Information Exchange (Model).

ph.06-RE.03
WHEREAS, [State Organization] is a health information exchange (HIE) organization formed for the purpose of facilitating HIE between and among providers, patients and authorized third-party entities. As part of this activity, [State Organization] allows participating providers who enter into and comply with this Agreement access to personal health information held by other participating organizations through the [State Organization] Network (the "Network").

ph.06-RE.03
Whereas, [State Organization] and Participant, together with certain other hospitals (and eventually together with additional hospitals, physicians, health plans, and others) intend to facilitate the electronic transmission, storage and sharing of health information amongst such participants in a manner that improves the quality, safety and efficiency of the delivery of healthcare through enabling the electronically interoperable delivery of clinical data to the point of care, while complying with all applicable laws and regulations, including without limitation those protecting the privacy and security of health information; and

ph.06-RE.03
Whereas, [State Organization] and Participant have decided to memorialize their respective rights and obligations as they relate to Participant's provision of data to and / or receipt of data from other participants, through [State Organization];

Now therefore, in consideration of the mutual promises hereinafter contained, and intending to be legally bound, [State Organization] and Participant do hereby agree as follows:

mm.09-RE.03
In an effort to encourage wider adoption of Electronic Health Records (EHRs) and establish a Health Information Exchange (HIE) network in [State] and throughout the United States, the national Health Information Security and Privacy Collaboration (HISPC) awarded a grant to the [State Organization] in conjunction with [State Organization] to develop a comprehensive marketing and public relations plan. The plan is focused on promoting the network’s benefit of exchanging critical medical information in a secure manner that ensures patient privacy. Toward that end, [State Organization] formed a communications advisory workgroup and queried its members for input as to how best to relay its message to stakeholders. The active workgroup contains members from several key groups, including physicians, patients, the state legislature, insurance companies and other payers, state and local government, medical records management, lawyers and project administrators.

mm.09-RE.03
Core Messages—Key Benefits of Electronic Health Records and Health Information Exchange

Improve Quality of Care: A network of Electronic Health Records ensures secure and timely access by providers to essential medical information when needed.

Improve Health Safety: Electronic Health Records and their exchange will reduce medical errors and unnecessary duplicate tests.

Reduce Healthcare Costs: EHRs will increase efficiencies through electronic charts and billing transmittals thereby decreasing paperwork and administrative costs.

Access to Care: An electronic health record network will be a strong physician recruitment tool, which will increase patient access to medical providers in [State].

Improve Health of [State]: Through the Personal Health Record, patients can choose to take an ownership role in their health care. A secure, online Personal Health Record will allow patients to review test results, prescription refills, and their medical records for accuracy.

Increase Patient Privacy and Security in exchanging Medical Records: The following safeguards will ensure greater privacy and security:

- Patient’s personal medical information will be shared through the network only with their permission.

- Prior to releasing any personal information, the identity of anyone using the EHR system will be carefully confirmed to prevent unauthorized access or cases of mistaken identity.
- Patients will have Internet access to review their own health and medical history via a secure account.
- Patients will be able to review who has accessed their personal medical information through the Personal Health Record.
- Employers will not have access to the secure network used to exchange information between healthcare providers.
- Special selected categories of the medical record will be protected from exchange.

mm.09-RE.03
Realizing the importance of identifying tangible, relevant benefits of EHRs to the patient, core messages also should emphasize the following real-life situations:

- Healthcare providers having access to current information in an emergency medical situation.
- Patients having access to their medical records when they are traveling out of state.
- Allowing patients access to their medical records when they visit their provider.
- Maintaining access to medical records during or after natural disasters when paper records may be lost or destroyed.

mm.07-RE.03
The purpose of this policy is to establish standards for identifying and verifying persons authorized to access the [State Organization] Health Information Exchange ([State Organization]). Proper identification of authorized persons (and exclusion of unauthorized persons) will ensure the privacy of protected health information accessible through [State Organization]. Additionally, adherence to this policy and procedure will ensure compliance with the identity verification requirements of the [State Organization] Provider Agreement.

pp.05-RE.03
Child Profile Information Sharing Insurance Co. Agreement

IV. The Insurer wishes to obtain access to the Information System in order to track Immunization Data pertaining to its Enrollees. HII wishes to make such information available to the Insurer, subject to the terms and conditions of this Agreement.

Regenstrief—Conformed Copy of INPC Second Participants Agreements

For a period of two (2) years after the termination of the Agreement as to all Parties, Regenstrief may continue to use the Information for scientific and research purposes, including, but not limited to, publication of research results in accordance with Article VII and Article VIII. After the two-year period, Participants may request that their Information no longer be used or disclosed for any purpose. Until such a request is made, Regenstrief may continue to use the Information in compliance with this Section, provided Regenstrief gives prior written notice to the affected Participants of any such use. Notwithstanding the foregoing, Information must continue to be stored on the Network for a longer period of time to the extent that Participants have agreed to make their Information available for research project approved pursuant to Article VII, in which case the Information shall continued to be stored, and may continue to be used and disclosed, for the duration of such research projects in compliance with the terms of the projects. After the applicable period discussed above, Regenstrief shall no longer use or disclose the Information for research purposes and the provisions of Article V (Confidentiality) and Article VIII (HIPAA Business Associate Provisions) shall continue to apply to the Information.

pp.05-RE.03
I. This is an agreement between the Health Information Institute, Inc., a [State] corporation ("[Entity]") and the partnership, corporation, limited liability company, or other private enterprise or government agency identified below ("Entity"), to provide for access to childhood immunization information contained in the [Name] Profile Immunization Registry and Tracking System ("[Name] Profile") by individual health care providers who are partners, officers, members, employees, or otherwise agents of or participants in the Entity ("Providers"), under which the Entity assumes the obligation to pay [Entity] the sums due for its Providers under their Individual Health Care Provider Information Sharing Agreements with [Entity].

ph.02-RE.03
6. Permitted Recipients and Users of Data. Only the following persons or entities may receive or use data subject to this Agreement.

ph.02-RE.03
a. PROVIDER/REPOSITORY may (i) use data subject to this Agreement to create limited data sets for purposes of this Agreement, and (ii) disclose data subject to this Agreement in limited data sets, to RESEARCHER or to a contractor expressly authorized in writing to obtain such data on behalf of RESEARCHER for purposes of this Agreement.

ph.02-RE.03
b. RESEARCHER may authorize a contractor to obtain and use limited data sets subject to this Agreement on its behalf, if the contractor has expressly agreed in writing to be bound by the terms and conditions of this Agreement.

ph.02-RE.03
c. RESEARCHER may authorize employees and agents to obtain and use limited data sets subject to this Agreement, upon their execution of an express written acknowledgment that they are or agreement to be bound by the terms and conditions of this Agreement.

ph.02-RE.03
d. An authorized contractor of RESEARCHER under this Agreement may authorize its employees and agents to obtain and use limited data sets subject to this Agreement if (i) they have been identified to and approved by RESEARCHER and (ii) they have executed an express written acknowledgment that they are or agreement to be bound by the terms and conditions of this Agreement.

sp.07-RE.03
ss.07-RE.03
Obtaining user access to [State] SIIS will provide me access to immunization information for children, in the State of [State].

sp.07-RE.03
Obtaining user access to the [State] SIIS will provide your facility access to immunization information for any person entered into the system.

sp.09-RE.03
The Data Sharing and Security Framework is designed to facilitate appropriate data sharing between and among organizations by addressing legal, regulatory, policy, proprietary, and contractual barriers to data exchange.

sp.09-RE.03
When fully developed, the Data Sharing and Security Framework will consist of policies, processes, model agreements, and other materials that participating centers agree to help develop and to adopt as appropriate. Together, these documents will cover critical issues such as the creation of a trust fabric for accepting user authentication credentials from other institutions, standards for the levels of security that are needed for different types of data, and suggestions on how to share data subject to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, as well as other applicable laws, regulations, and policies.

sp.09-RE.03
This document provides an overview of the Data Sharing and Security Framework. It outlines what tools may be included in this bundle, their specific function, and the role participating cancer centers are expected to play.

sp.09-RE.03
The Data Sharing and Security Framework promotes the National Cancer Institute's overarching goal to connect the people, institutions, and data in the cancer community through [State Organization]. This collection of tools and capabilities is one of three "bundles" that have been designed to help support and streamline clinical trials, imaging, tissue banking, and integrative cancer research, and to provide the materials needed to join the secure [State Organization] data-sharing framework.

mm.10-RE.03
In the immediate aftermath of the September 11, 2001 terrorist attacks, one of the many initiatives undertaken by state governments across the nation was to begin comprehensive reviews of state law, agreements and protocols dealing with emergencies. State and territorial health officials played a unique role in these processes through their identification and definition of the central importance of public health issues, expertise and approaches in emergency planning, preparedness and response at all levels of government: local, state, territorial and federal.

Four years into the enterprise of re-envisioning public health's emergency preparedness and response capabilities and responsibilities, many state public health laws, regulations and procedures have been newly developed or extensively revised. The public health workforce has been challenged to embrace new competencies and missions. With these efforts has come a growing awareness of the magnitude of the potential threats to the public's health and, therefore, also the need for public health professionals from all jurisdictions to work together through sharing information, resources and expertise. All states are interdependent and public health emergencies do not respect borders. State health officials have recognized that the public health system must be prepared in all jurisdictions at all times.

Success brings new challenges. As states and local jurisdictions have been confronted with the challenge of working across jurisdictional lines in the cause of public health preparedness, so they are now increasingly confronted with the challenge of working across national boundaries. In the spring of 2005, the Association of State and Territorial Health Officials (ASTHO) and its Preparedness Policy Committee requested that a work group be established to examine cross-border public health preparedness and attendant legal issues.

Working in concert with experts from the Johns Hopkins Bloomberg School of Public Health, this work group identified two basic resources that would assist with cross-border public health preparedness efforts: (1) an introduction to the law governing the formation of cross-border agreements by the states; and (2) a draft template for a "public health annex" to existing, international mutual assistance agreements. Both documents were initially presented for feedback at a meeting of northern border states that was held in [City], [State] on May 16, 2005.

These resources are intended to serve as a tool to assist states in public health planning, preparedness and response across both sides of the United States' borders in a common effort to protect the health of the U.S. population and that of its neighbors in the Americas. These briefing documents are by no means an exhaustive review of all of the legal issues and should be considered only as a starting point for discussion.

mm.10-RE.03
ASTHO commissioned this short summary. Its purpose is to begin an exploration of the legal rights and restrictions of the States as they consider entering agreements with sovereign entities outside the United States of America ("foreign sovereigns"). The conclusions and statements contained herein are not ASTHO's and have not been endorsed by ASTHO.

Topics introduced include the scope of states' authority under the United States constitution; the parameters of that authority as described in some of the case law; and federal legislation and/or policy bearing on the formation of agreements between the states and foreign sovereigns.

It must be noted that this briefing paper concerns itself with "cross-border" agreements—agreements with foreign sovereigns that are territorially contiguous with the United States (i.e., Mexico and Canada). Some of the considerations discussed below may apply only to "cross-border" agreements.

mm.10-RE.03
The signatories recognize that in order to safeguard the health of their populations and facilitate emergency preparedness and response their respective agencies or ministries charged with the protection of public health should exchange individual and/or population-level (epidemiological) health data.

Purpose of disseminating health data

mm.10-RE.03
The signatories recognize that optimal management of a public health emergency may require the movement or retention of evacuees and/or refugees into, out of or across their respective jurisdictions. The signatories desire to facilitate such actions subject to the governing laws and regulations by which they are bound. [PNEMA p. 3, ¶3(c)]

mm.10-RE.03
In the event that a signatory requests the assistance in its jurisdiction of other signatories in making available health care personnel to prevent, detect or respond to a public health emergency, the signatories intend that the following will apply. Annex outside the sending signatory.

mm.10-RE.03
The signatories pledge their commitment to a relationship of continued cooperation and support in emergency planning and management. To this end the signatories agree to

undertake the following planning activities within the next 6 months or at such other time as the signatories agree.

ph.09-RE.03
1.2 Purposes. The purposes for which the SNO is organized.

ph.06-RE.03
Introduction. This document (“Model”) is a model for the organization and content of the Terms and Conditions of a sub-network organization (“SNO”).

ph.02-RE.03
1. Data to be Made Available. Subject to compliance with this Agreement, Data Provider authorizes PROVIDER/REPOSITORY to make Limited Data Sets available to RESEARCHER from data hosted by PROVIDER/REPOSITORY on the Data Provider’s behalf, for use in research testing BIOSURVEILLANCE. Each Limited Data Set may include the data elements set forth in Appendix A.

ph.06-RE.03
Although [State Organization] is not a Covered Entity, this Agreement is entered into for the purpose of protecting the confidentiality and security of patient information transmitted or communicated to the above Patient as part of or in connection to the Network and for complying with the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, 45 C.F.R. Parts 160 and 164 (“HIPAA”).

ph.09-RE.03
Use of Model. The Model is based on a number of assumptions, which are described in the following discussion. The Model is not the “answer” for all SNOs. Instead, it is intended to assist in the organization of a SNO by providing a basis upon which to begin drafting that SNO’s Terms and Conditions. All language provided in the Model is intended for informational and educational purposes only. It is not intended, nor should it be used, as a substitute for legal advice. In preparing its own terms and conditions, or other legal documents used in connection with its participation in the NHIN, an organization should consult with legal counsel. Each SNO will have to draft its Terms and Conditions based upon its own organization, operations, system and services, regulatory environment, and so on. Some of the Model’s terms will be inapplicable to some SNOs. The Model shows where some of the variations might be expected to occur.

Overview of Structure

ph.09-RE.03
Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the “Common Framework Policies and Procedures.” The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

ph.06-RE.03
Use of Model. The Model is based on a number of assumptions, which are described in the following discussion. The Model is not the “answer” for all SNOs. Instead, it is intended to

assist in the organization of a SNO by providing a basis upon which to begin drafting that SNO's Terms and Conditions. All language provided in the Model is intended for informational and educational purposes only. It is not intended, nor should it be used, as a substitute for legal advice. In preparing its own Terms and Conditions, or other legal documents used in connection with its participation in the NHIN, an organization should consult with legal counsel. Each SNO will have to draft its Terms and Conditions based upon its own organization, operations, system and services, regulatory environment, and so on. Some of the Model's terms will be inapplicable to some SNOs. The Model shows where some of the variations might be expected to occur.

sp.06-RE.03
In order to secure data that resides in a CMS Privacy Act System of Records, and in order to ensure the integrity, security, and confidentiality of information maintained by the CMS, and to permit appropriate disclosure and use of such data as permitted by law, CMS and enter into this agreement to comply with the following specific paragraphs.

ph.06-RE.03
Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the "Common Framework Policies and Procedures." The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

mm.09-RE.03
1. Introduction

In 2002, within the framework of the Health Working Group of the US-Mexico Binational Commission, representatives from the U.S. Department of Health and Human Services and Mexico's Secretaria de Salud established a binational group on Epidemiologic Surveillance and Information Exchange to address issues of interest to both countries. With the objective of better defining how the two countries should collaborate on epidemiologic events of mutual interest, this binational group has elaborated the present document to provide a set of common guidelines.

mm.09-RE.03
The United States and Mexico have a rich tradition of collaboration on epidemiologic events involving the two countries, including infectious disease outbreaks, diseases associated with products from the other country, and the continuity of care for patients with tuberculosis traveling between the two countries. A joint Border Infectious Disease Surveillance project has been in place for several years, and an Early Warning Infectious Disease Project was initiated in 2004. The Binational TB Card Project facilitates healthcare provider access to information on TB patients traveling between the two countries to ensure continuity of therapy. Closely linked to these collaborations, public health professionals from the two countries have regularly sought to keep their counterparts apprised of relevant epidemiologic events.

mm.09-RE.03
However, clear standards have not yet been established for what information should be shared and how the sharing should take place. The Core Group on Epidemiologic Surveillance and Information Sharing of the US-Mexico Binational Commission Public Health

Working Group has chosen to formulate such a set of guidelines with the objectives of better institutionalizing the exchange of information on epidemiologic events of mutual interest, and promoting collaborative responses when appropriate. Recognizing that productive collaboration already occurs between many 'Sister Cities' along the US-Mexico border and between neighboring states, it should be emphasized that the present Guidelines for US-Mexico Coordination on Epidemiologic Events of Mutual Interest (Guidelines) should facilitate continued existing binational cooperation, while at the same time fostering more systematic and comprehensive sharing of information at all levels of government. These Guidelines focus primarily on coordination between the public health agencies/units which have primary responsibility for epidemiologic surveillance. They do not seek to define coordination between agencies/units with major regulatory functions, for which agreements have already been established.

mm.09-RE.03
These guidelines are emerging shortly following the adoption by the World Health Assembly on May 23, 2005 of the International Health Regulations (IHR), designed to "better respond to the increasing interaction between countries of the world, and to the changing nature of public health threats." The Guidelines directly address IHR Article 44—Collaboration and Assistance—which affirms that "State Parties shall undertake to collaborate with each other" for identifying, investigating and responding to events, for providing technical and logistic support, and in other ways. However, the present document extends beyond the scope of the IHR—which targets public health emergencies of international concern—by presenting guidelines for the sharing of epidemiologic information between the two countries regarding all epidemiologic events of mutual interest. It is not limited to public health emergencies of international concern, but seeks to maximize the capacity of each country to respond to all epidemiologic events of mutual interest.

mm.09-RE.03
General Principles which orient the Specific Guidelines

The Legal Framework for such binational coordination The Scope of Epidemiologic Events to which these guidelines are meant to apply Specific Guidelines for different classes of epidemiologic events These Guidelines are meant to serve as a standard of conduct for public health agencies and their staff in responding to epidemiologic events of shared interest to both countries. While the Guidelines are not binding, it is planned they will lead to the development of shared protocols to facilitate their full implementation.

mm.09-RE.03
2. General Principles

The guidelines of this document are based on the following principles:

2.1. The Need to Share Information

The primary mission of public health agencies of the US and Mexico is to protect and promote the health of their citizens. However, epidemiologic events involving both countries—by geographic proximity, by cross-boundary movement of their citizens, or by exchange of their products—require the sharing of information between counterpart institutions. Such sharing has the objectives of providing information about potential risks and facilitating an appropriate response for the protection of the health of the public, in whichever country they reside. Adequate preparation for the risks of bioterrorism or other public health emergencies further requires that well-functioning channels of communication be established prior to the occurrence of such an event, to facilitate effective sharing of crucial information, and articulation of coordinated responses, to ensure the greatest protection possible of the public's health.

mm.09-RE.03
In addition to sharing information to directly protect the public's health, counterpart agencies are also expected to share information on other public health matters affecting both countries, such as revised policies on travel or imported products from the other country. Such alterations in one country's positions will create important demands on the public health agency of the other country, for which they should be as well prepared as possible to respond.

mm.09-RE.03
2.6. Differences between Health Systems

The roles of public health agencies of the United States and Mexico at the different levels of government are not always the same. In the United States, the public health sector is primarily state-based, while Mexico's health system is more centrally directed by the national Secretaria de Salud. Such differences must be taken into consideration in mounting the necessary responses when the two countries face an epidemiologic event requiring collaboration.

mm.09-RE.03
5.2.1. Foodborne Disease Outbreaks

Foods are responsible for many infections and toxic exposures. Within the United States foodborne diseases are estimated to be responsible annually for 76 million illnesses and 5000 deaths. The growing international trade of agricultural products has correspondingly been associated with outbreaks due to pathogens transmitted by foods imported from another country. The United States and Mexico have collaborated in responding to several such outbreaks.

mm.09-RE.03
The organization of governmental roles in food safety often includes multiple agencies in both the health and agricultural sectors, and at the federal, state and local levels. To facilitate needed collaboration, a clear definition of the different roles of such agencies needs to be understood by neighboring countries, including the responsibility of each in responding to outbreaks of foodborne diseases.

mm.09-RE.03
The complexity of institutional organization on food safety in both countries creates an important need for collaboration between federal, state, and local authorities across international borders.

mm.09-RE.03
Foodborne disease outbreaks often imply the need for two or more stages of investigation. The first stage is the primary epidemiologic and environmental investigation which ideally will identify the agent, the food vehicle and how the food became contaminated. Traceback of the food vehicle will indicate whether it is a domestic or imported product. In the latter case, and if the food product is suspected to have been contaminated at its point of origin, further traceback investigation of the implicated food product will determine its source. Additional investigation may identify how the food product became contaminated, where the most effective opportunity for future prevention exists and the need for regulatory action.

These investigations represent important opportunities for collaboration between the two countries.

mm.09-RE.03
5.3 Potential Terrorist Events

Recent events have forced the United States to recognize that intentional use of biologic, chemical or radiologic/nuclear agents to harm people of this country is a risk which it must be prepared to face. The possibility of introduction of such agents by way of the US-Mexico border or the release of an agent in one country with transmission to the other makes this an issue of interest to both countries. Such a scenario could foresee the appearance of cases in the border region which would require close binational coordination.

mm.09-RE.03
The suspicion or identification of such an event as being intentional would lead to the involvement of law enforcement and potentially other agencies outside the health sector, with which national public health agencies would need to cooperate, as defined in national emergency response plans.

mm.09-RE.03
Since disease arising by intentional spread may well appear without previous notice, health officials need to be aware of suggestive features of such an incident, including the following:

- An outbreak of an unusual syndrome or disease, compatible with agents associated with bioterrorism, especially when occurring in a discrete population.
- Many cases of unexplained diseases or deaths.
- More severe disease than is usually expected for a specific pathogen or failure to respond to standard therapy.
- A disease that is unusual for a given geographic area or transmission season.
- Multiple simultaneous or serial epidemics of different diseases in the same population.
- Unusual strains or variants of organisms or antimicrobial resistance patterns different from those circulating.
- Similar genetic typing of agents isolated from distinct sources at different times or locations.
- Intelligence of a potential attack, claims by a terrorist or aggressor of a release, and other evidence suggesting terrorist intent.
- Other unusual situations

mm.09-RE.03
5.4 Laboratory Issues

Laboratories serve a unique role in both surveillance and investigation of health problems. The purpose of this section is to establish guidelines for laboratories when significant health events of binational interest occur mandating a collaborative response by both nations.

mm.09-RE.03
The availability of laboratories and the complexity of testing which those laboratories are capable of performing vary along the length of the border in the two countries. This may

lead to periodic use of laboratories by border clinicians or patients in the neighboring country. In addition, disease outbreaks or emergency preparedness plans may lead to decisions to share laboratory resources. In such cases, minimizing the time required for laboratory diagnosis and confirmatory testing is critical to timely identification of health problems and disease outbreaks so that appropriate and timely control measures can be implemented. This is particularly important when considering bioterrorism events and outbreaks of highly communicable diseases such as pandemic influenza or Severe Acute Respiratory Syndrome (SARS) which have the potential to cause substantial health, social, and economic problems.

mm.09-RE.03
Each of the specific items detailed below must be addressed in establishing an efficient, highly functional, binational framework for laboratories to develop the needed capabilities for responding capably to disease outbreaks and other health challenges impacting both countries.

RE.04 Miscellaneous Recitals Provisions

ph.06-RE.04
Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the "Common Framework Policies and Procedures." The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

ph.09-RE.04
Common Framework Policies and Procedures. The Model assumes that the NHIN will be implemented in accordance with a compilation of documents to be known as the "Common Framework Policies and Procedures." The Common Framework Policies and Procedures will describe how the NHIN works and will include certain terms that should apply to all SNOs. The Model makes a number of assumptions about the future structure and content of the Common Framework Policies and Procedures, which are identified throughout the document. The Model should be revisited and revised as necessary to work with the Common Framework Policies and Procedures as they develop.

ph.09-RE.04
SNO Terms and Conditions. The Model assumes that each SNO will adopt its own "Terms and Conditions" which will be comprised of terms that apply to that SNO only, and will also incorporate the provisions of the Common Framework Policies and Procedures that apply to all SNOs.

ph.09-RE.04
Registration and Registration Agreements. The Model assumes that Participants will receive access to the SNO's Services and/or access to the SNO's System by registering with a SNO and entering into a "Registration Agreement." The Registration Agreement will incorporate the SNO Terms and Conditions by reference and will require the Participant to comply with those parts of the Terms and Conditions that apply to the Participant, based on how the Participant uses the SNO's Services and/or System.

sp.09-RE.04
Achieving technical interoperability in and of itself will not deliver the full benefits of accelerated translational research and expedited care for the patient. These are only possible when researchers and oncologists have the information they need to do their work better. However, there are very important non-technical considerations, such as patient privacy protections and intellectual property interests, which affect the ability to make data available.

pp.06-RE.04
Section 2.01 Replacement of First Agreement. The Parties previously entered into the First Agreement, and now wish to update and restate the First Agreement through this Agreement. The Parties desire this Agreement to supersede and replace the First Agreement. The First Agreement was created in the context of a specific contract with the National Library of Medicine to study the effects of city-wide sharing of health information used in emergency rooms and in primary care on the cost of health care and the efficacy of treatment for patients. Its scope of usage was limited to emergency room encounters and primary care encounters and to clinical information held by the Participants that would be useful for the care of patients during those encounters. Since that time, the Participants have agreed to allow their Information to be used for additional research purposes, most notably the [Name] Network which seeks to create a Web-based system capable of searching existing electronic databases, such as the Network, to locate human specimens and associated clinical and pathologic data needed for cancer research. At Management Committee meetings, Participants have expressed an interest in broadening the Network to care providers in settings such as the hospital or the group practices for treatment purposes.

pp.06-RE.04
Section 2.02 Purposes of Second Agreement. The Participants desire to continue and expand their participation in the Network by storing Information on the Network, allowing Full Participants access to such Information, and/or retrieving patient data from the Network in order to provide informed health care to their patients consistent with letters of intent and other commitments the Participants have made since the execution of the First Agreement to submit additional Information to the Network and participate in research projects related to the Information.

The Parties recognize the benefits in increased quality of patient care to be gained from the sharing of patients' medical information. Through the sharing of health information of patients who are seen by more than one of the Participants, the Network seeks to reduce the costs of care inefficiencies such as unnecessary repeat testing and increase the accuracy of medical diagnoses through common and rapid access to patient information through electronic means to lead to improved outcomes for patients.

The Parties further recognize the enormous opportunities to utilize the broad-based and ever-growing collection of Information on the Network for research purposes related to, among other things, studying the efficacy and cost-reducing effects of broad-based access to patient information and reviewing the Information to learn about specific diseases and their treatment.

Since the execution of the First Agreement, the Privacy Rule issued under the Health Insurance Portability and Accountability Act of 1996 has clarified the responsibilities and agreements that must exist to protect the privacy of PHI and simplified the requirements for sharing such information for Treatment purposes. In addition, new grants and contracts have been awarded in which some or all of the Participants are involved that allow for an expansion of the information that the Participants wish to share among one another and for research purposes. The Privacy Rule gave organizations with existing data sharing contracts (such as the First Agreement) until April 14, 2004 to create a new agreement that follows the HIPAA requirements for business associate agreements. Because the First Agreement contemplates the use and disclosure of Information for both treatment and research purposes, it is necessary to revise the First Agreement through this Agreement to ensure that the Network's use and disclosure of Information operates within the framework created by the Privacy Rule.

ph.02-RE.04
a. The parties acknowledge that the Data Provider is (i) a Covered Entity, as that term is defined in the Standards for Privacy of Individually Identifiable Health Information published by the United States Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), codified at 45 CFR § 164.103, and (ii) a health care provider as defined in REDACTED; and that compliance with HIPAA and STATE LAW is of the essence of this Agreement.

ph.02-RE.04
b. The data made available to RESEARCHER by the Data Provider under this Agreement is intended to be provided in "limited data sets" within the meaning of that term in the Limited Data Set Standard of the Standards for Privacy of Individually Identifiable Health Information published by the United States Department of Health and Human Services, codified at 45 CFR § 164.514(e)(2).

ph.02-RE.04
c. This Agreement shall interpreted as a "data use agreement" within the meaning of that term in the Limited Data Set Standard of the Standards for Privacy of Individually Identifiable Health Information published by the United States Department of Health and Human Services, codified at 45 CFR § 164.514(e)(4).

ph.02-RE.04
d. No limited data set shall be provided under this Agreement which includes any information that identifies or can readily be associated with the identity of the patient, in order to avoid the provision of [REDACTED].

ph.06-RE.04
SNO Terms and Conditions. The Model assumes that each SNO will adopt its own "Terms and Conditions" which will be composed of terms that apply to that SNO only, and will also incorporate the provisions of the Common Framework Policies and Procedures that apply to all SNOs.

ph.06-RE.04
Registration and Registration Agreements. The Model assumes that Participants will receive access to the SNO's Services and/or access to the SNO's System by registering with a SNO and entering into a "Registration Agreement." The Registration Agreement will incorporate the SNO Terms and Conditions by reference and will require the Participant to comply with those parts of the Terms and Conditions that apply to the Participant, based on how the Participant uses the SNO's Services and/or System.

sp.06-RE.04
Directions for the completion of the agreement follow:
Before completing the DUA, please note the language contained in this agreement cannot be altered in any form.

First paragraph, enter the Requestor s Organization Name.

Item #1, enter the Requestor s Organization Name.

Item #4, enter the Custodian Name, Company/Organization, Address, Phone Number (including area code), and E-Mail Address (if applicable). The Custodian of files is defined as that person who will have actual possession of and responsibility for the data files. This section should be completed even if the Custodian and Requestor are the same.

Item #5 will be completed by a CMS representative.

Item #6 is to be completed with the Study and or Project Name and a brief description of the purpose for which the file(s) will be used.

Item #7 should delineate the files and years the Requestor is requesting. Specific file names should be completed. If these are unknown, you may contact a CMS representative.

Item #8, complete by entering the Study/Project s date of completion.

Item #15 will be completed by CMS.

Item #19 is to be completed by Requestor.

Item #20 is to be completed by Custodian.

Item #21 will be completed by a CMS representative.

Item #22 should be completed if your study is funded by another Federal Agency. The Federal Agency Name (Other than CMS) should be entered in the blank. The Federal Project Officer should complete and sign the remaining portions of this section. If this does not apply, leave blank.

Item #23 will be completed by a CMS representative.

Once the DUA is received and reviewed for privacy issues, a completed and signed copy will be sent to the Requestor for their files.

sp.06-RE.04
This Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (DHHS), and, hereinafter termed "User."

sp.02-RE.04
The parties therefore wish to provide for compliance with such laws in this Agreement and in the policies and procedures administered by the [Program] Management Committee.

sp.02-RE.04
9. Effect on Existing Agreement.

If the Participant is already participating in [Program], entry into this Agreement shall effect an amendment of the existing Agreement, and shall not terminate the Agreement.

mm.10-RE.04
This White Paper proposes a new template that should be used when defining policies for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a

particular nation or region. This template provides a consistent documentation format for specifying implementation decisions, policies, and possible refinements of XDS and related Profiles. Additionally, its' outline provides a comprehensive list of all relevant topics that XDS Affinity Domain implementers may find helpful in planning for deployment.

mm.10-RE.04
Goals

This paper addresses the following goals:

- Describe the issues to consider when planning the deployment of XDS Affinity Domains.
- Define the areas of the XDS and related Profiles to consider refining for XDS Affinity Domains.
- Provide a standardized document template to be used when specifying the deployment policies for a single XDS Affinity Domain, or for multiple XDS Affinity Domains that are in a particular nation or geographic region.

mm.10-RE.04
Request for Feedback

The IHE IT Infrastructure Technical Committee requests feedback on the concepts described in this White Paper. In particular, we would like your thoughts on whether this paper addresses all the issues involved and what you think of the proposed organization of this template.

Comments arising from Trial Implementation may be submitted to http://forums.rsna.org under the forum:
"IT Infrastructure Technical Framework "

Select the sub-forum:
"Template for XDS Affinity Domain Deployment Planning"

The IHE ITI Technical Committee will address these comments and publish a Trial Implementation version of this template in August 2007.

mm.10-RE.04
Open Issues and Questions
Overview

Currently, ITI TF Appendix L provides an informative checklist for the key policies that need to be addressed in order to deploy an EHR-LR document sharing environment for an XDS Affinity Domain. However, it has been recognized that this existing checklist is incomplete. Many additional implementation details may need to be defined, depending upon the scope of the XDS Affinity Domain in question and the degree to which particular rules are to be defined (i.e. for architecture, content, security, etc.). This White Paper proposes a new template that should be used when defining policies for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a particular nation or region. It takes the form of a template rather than a checklist because it acts more as an outline for all the issues that should be considered, rather than a checklist to be used to verify the correctness of a particular implementation. It is proposed that the checklist in ITI TF Appendix L will be replaced by a brief summary of the content of this White Paper, along with a reference to it.

mm.10-RE.04
It is realized that not all of the items in this template will need to be defined for every XDS Affinity Domain, or at every national or regional level. The list of items that need to be defined will depend upon the scope of the specifications, and whether they are for a particular XDS Affinity Domain, region, and/or nation.

mm.10-RE.04
When defining the policies and Profile refinements for an XDS Affinity Domain it is essential that these do not contradict those mandated for all XDS Affinity Domains in the particular nation or region in which the XDS Affinity Domain will exist. In addition, these specifications for a particular XDS Affinity Domain should not duplicate those defined at a larger regional or national level. Instead the documentation for the particular XDS Affinity Domain should reference the document defining the national or regional policies.

mm.10-RE.04
Introduction

Define introductory text specifying the nature of the XDS Affinity Domain, or organization, region, or nation for which the XDS Profile extensions apply. If XDS Profile extensions are being defined at a national or regional level and are meant to be followed by all XDS Affinity Domains within them then this should be clarified here. The people and organizations involved in creating these should be specified, as well as any professional or regulatory organizations that were involved in their creation and/or have approved them.

mm.10-RE.04
If the XDS Affinity Domain extensions are being defined at a national level and there is an official IHE organization for the country involved then this organization must approve the extensions and this must be stated here. It is the responsibility of the national committee involved to determine whether testing of the extensions is necessary before they can be approved. It is still possible for national extensions to be defined for a nation that does not have an official IHE organization, however it will be necessary for the organization(s) proposing these extensions to demonstrate that they have the authority to actually define such extensions.

mm.10-RE.04
Reference Documents

List of all documents that are referenced in the XDS Affinity Domain 1extensions or were used as input in some way to the creation of these extensions.

mm.10-RE.04
Membership Rules
Acceptance

Define the types of organizations and individuals that can become members of the XDS Affinity Domain so that they will be permitted access to its components and data. Specify how they can apply for membership.

mm.10-RE.04
If there are any different rules for handling the membership of organizations and individuals whose physical location is considered part of another XDS Affinity Domain then define these here. For example, if the XDS Affinity Domain is defined for a specific geographic region, such as a Province or State, but an organization or individual located outside of this region

wants to become a member. In addition, if there are any special rules for handling the membership of organizations and individuals who are already members of a different XDS Affinity Domain then define these here also.

mm.10-RE.04
Types of Membership

Are there different types of membership that define how published data can be accessed (i.e. read-only, publish-only, etc.)? How will it be ensured that members are only permitted this type of access?

mm.10-RE.04
Membership Policies

Define any rules regarding management of member's status. How does an individual or organization apply to no longer be a member? How is the list of members maintained and distributed? Is the list of member's public? If not then what is the policy regarding requests for access to this list? Handling of membership in multiple XDS Affinity Domains.

ph.06-RE.04
WHEREAS, Network has entered into an agreement with ______________________ ("Access Provider") under which Access Provider has agreed to provide Network's designated "registered users" with access to the Exchange to view patient information generated by participating health care providers ("Data Providers"); and WHEREAS, Network has entered into an agreement with ___________________ ("Host") to host the Exchange; and

sp.08-RE.04
State and Clinic hereby agree to this Memorandum of Understanding (MOU) concerning Clinic's use of a computer and software provided by the State for entering immunization information into the [State] Immunization Information System ([IIS]). This MOU replaces any and all previous MOUs entered between the parties regarding the [State IIS]. This MOU begins the day both computer and software are installed and terminates December 31, 2007. This MOU can be terminated upon 30 days written notice being received by the other party and may be terminated for cause by State at any time with or without notice.

mm.06–RE.04
Vision. The Exchange's vision is to develop and maintain an electronic health information system that provides a longitudinal electronic medical record for __________________ patients that can be accessed and updated in real time by authorized health care providers.

sp.08 RE.04
Standards for Transactions.

Minimum Necessary Information. Prior to conducting any Transaction in which Protected Information is Disclosed, the parties shall establish the Minimum Necessary Information for purposes of that Transaction.

Specifications Addenda. Prior to conducting any Transaction subject to this Agreement the parties shall enter into a Specifications Addendum applicable to that Transaction. Any Specifications Addendum shall include the following provisions:

- An identification of the parties.
- A statement incorporating this Agreement by reference.

- A description of the purpose(s) for which Protected Information will be Disclosed in the Transaction.[12]
- A description of the scope of the Protected Information which will be Disclosed.[13]
- A description of the Uses and Disclosures permitted with respect to Protected Information Received.[14]
- A description of the format(s) in which information will be disclosed.
- A description of the method(s) by which information will be Transmitted, including encryption or other technical security mechanisms implemented if using electronic communications network.
- If an Intermediary will be used, it must be identified.
- A description of the means used to Authenticate person(s) Authorized to Receive Protected Information.
- The parties may elect to state additional or more detailed requirements for the Protection of information.
- If the purposes for the Disclosure include Anonymizing or Aggregation of Protected Information, that must be stated.
- If the parties wish to implement Electronic Signatures and/or Electronic Records, the applicable procedures and processes for Electronic Signatures must be specified and the Electronic Records Warehouse must be identified.
- While not required, it may be desirable to include terms for payment of fees or other applicable sums payable in connection with Transactions under this Agreement.

4.3 Statement of Relationship (SR)

mm.10-SR.00
The sending signatory is responsible for the cost of transportation, the health and safety of evacuees and/or refugees while in transit and the cost of supplies and equipment used in transport unless otherwise agreed. Each signatory is responsible for the maintenance of its own supplies and equipment used in transportation unless otherwise agreed. Movements of evacuees and/or refugees pursuant to this Annex shall be by the most expeditious means available, including but not limited to the use of a sending signatory's emergency vehicles not ordinarily authorized for use in the jurisdiction of a receiving signatory.

mm.10-SR.00
The signatories agree to use their best efforts to ensure that evacuees and/or refugees transported from other signatories to their territories receive emergency health and social services in a manner no less favorable than their own citizens. [PNEMA p. 3, ¶3(d)] In addition, the signatories agree that evacuees and/or refugees shall be provided safe and adequate shelter, food, clothing and means of communication as necessary, commensurate

[12] This statement is required in order both to document the authority for the Disclosing Party's Disclosure, as required by the Privacy Rule at 82,805, 45 CFR sec. 164.502(a), and to define and limit the Receiving Party's authority to Use or further Disclose Protected Information, as required in the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)2)(i).

[13] This description is intended to document that the Disclosure is of the "Minimum Necessary" information, as required in the Privacy Rule.

[14] This is a required element of a Business Associate Contract under the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(i).

with the conditions under which the receiving signatory's citizens are provided for. A sending signatory's personnel shall be given access to evacuees and/or refugees, records relating to them and the premises where they are housed and/or fed on the same basis as the receiving signatory's personnel.

ph.09-SR.00
1.1 Nature of Organization. The legal structure within which the SNO is organized, and the SNO's essential relationships to sponsors, founders and others.

ph.06-SR.00
1.1 Nature of Organization. The legal structure within which the SNO is organized, and the SNO's essential relationships to sponsors, founders, and others. [Name of SNO] ("[SNO Name]") is [insert type of organization and state in which organized, e.g., a [State] public benefit corporation], organized by [insert description of founders, sponsors, etc.]. [SNO Name] is a participant in the National Health Information Network ("NHIN").

mm.10-SR.00
Organizational Structure

Describe the organizational structure within the XDS Affinity domain. Considerations include, but are not limited to:

Organization of XDS Affinity domain governance (options to consider include: central point of authority, collaborative governance, distributed governance, etc.).

List the founders, controllers, administrators, etc. of the XDS Affinity Domain. Their roles and responsibilities should be clearly defined, and contact information provided. It should be made clear who someone wishing to participate in the XDS Affinity Domain should have to contact in order to obtain information regarding participation in or access to the XDS Affinity Domain.

sp.04-SR.00
This Participating Clinic Agreement is entered into by and between the [State] Department of Health, [Name] Breast and Cervical Cancer/Chronic Disease Screening Program, hereinafter referred to as [Program], and ______________________________, hereinafter referred to as Participating Clinic. This Agreement replaces any previous Agreement between the parties and is intended to incorporate requirements of the Health Insurance Portability and Accountability Act, 45 C.F.R. Parts 160 and 164 (HIPAA). Participating Clinic is an independent contractor and is responsible for maintaining professional liability insurance coverage and all other obligations related to Participating Clinic's independent service provision status.

"Participating Clinic," as used in this agreement, shall mean the independent contractor listed above, for the purpose of providing services authorized by [Program], whose staff are licensed: (1) as a physician by either the State of [State] Board of Medical and Osteopathic Examiners or the state in which the physician practices; or (2) by the State of [State] or the state in which they practice to provide services including, but not limited to, medical, laboratory, radiological, hospitalization, pharmacy, and/or related health services

mm.09-SR.00
2.5. Joint Action to Respond to an Epidemiologic Event

When an epidemiologic event occurs involving both countries and both have an interest in investigating the event (such as an outbreak investigation), the two countries should make a determined effort to conduct the investigation together. In this situation, the national public health agency of the country in which the study will take place has jurisdiction and will assume the coordinating role. Each country should be expected to provide the technical and financial support needed for its participation. Sharing of resources, e.g., laboratory testing, may be necessary, is highly encouraged, and should be negotiated in a timely fashion. The timeliness of the investigation should be accorded a high priority by both countries. When rapid action is appropriate, the deployment of the team in the country where the outbreak is occurring should not be slowed by the delayed mobilization of the corresponding team from the other country.

mm.09-SR.00
There is a tremendous interaction between the U.S. and Mexico in the Border region, reflected by the more than 242 million northbound passenger crossings registered in 20043. While the physical proximity and intense interaction of the two countries in the Border region raises the risk of shared exposure to disease-causing agents by citizens from both countries, binational travel and commerce are capable of carrying such exposures far beyond the border. The potential of an epidemiologic event to be binational must be considered throughout the full reach of both countries.

mm.09-SR.00
Upon recognition of a binational outbreak, if new cases continue to appear or exposure to causal agents persists, a rapid response is needed to accurately diagnose the illness, to determine the scale of the outbreak, to identify significant risk factors, and/or to implement appropriate control measures. Coordination between public health agencies of the two countries is essential for meeting the needs of all relevant parties and to achieve the most effective use of available resources.

ss.08-SR.00
Some or all of the information to be disclosed is required by law to be protected against unauthorized use, disclosure, modification or loss. A violation of such a legal requirement may lead to criminal or civil penalties or other harm or damages. In order to comply with applicable legal requirements for the protection of information, the parties agree as follows.

WHEREAS the [State Department], Division of [State Department] – [State Program] and the [State Office] and the [City Department] through the [State] Department of Health (collectively, "the parties") wish to engage in a data sharing/data exchange pilot test of immunization data that is housed in the immunization registry systems of [State] and the [City] with the goal of confirming that data sharing and data exchange can occur between states and across state lines using electronic technology; and

ss.08-SR.00
NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

I. Under this Agreement, the [State Department], DOH and the DOH shall not provide nor exchange funding to one another for the pilot test. Each of the Participants will absorb the cost of said pilot test. Hereinafter the above shall be referred to as "the Participants:"

ss.08-SR.00
The primary technical leads for the pilot test are:

The technical leads will develop the technical specifications for the data exchange project, file specifications, program modifications to existing applications, operational environments and schedules, help desk documentation and training, patient matching criteria, and so forth.

ss.08-SR.00
The non-technical members of the team are:

Project Oversight:

ss.08-SR.00
2. Each of the participants is an independent entity and neither party shall hold itself out as an agent, partner or representative of the other.

4.4 Recipient Requirements (RR)

RR.01 Acceptance of Grant of Right/License to Use the HIE

ph.02-RR.01
5. Limitation of Intellectual Property Rights. The only intellectual property rights provided by this Agreement are (i) a license to PROVIDER/REPOSITORY to use data to create limited data sets for disclosure to RESEARCHER under this Agreement, and (ii) a license to RESEARCHER to use the limited data sets obtained from PROVIDER/REPOSITORY for research purposes under this Agreement. These limited licenses shall terminate upon the termination of this Agreement for any reason.

hh.06-RR.01
2. Network License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, each Network is hereby granted a limited license to allow its Authorized Users via their Registered Users to remotely access and use the Exchanges and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by the Networks.

SP.06-RR.01
The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and the person will be responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time

ph.06-RR.01
5.2 Certification of Authorized Users. How the Participant will provide assurances that its Authorized Users have been trained appropriately. At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User: (a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training); (b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type); (c)

Has agreed not to disclose to any other person any passwords [and/or other security measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms); (d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and (e) [Others, if desired].

ph.06-RR.01
4.3.3 Approval and Disapproval of Registration Forms. The SNO will be entitled to review all registration forms and decide not to accept any given party's registration. [SNO Name] shall review each Registration Form and shall approve or disapprove each in accordance with the Terms and Conditions and as [SNO Name] determines in its sole discretion is appropriate. [SNO Name] shall not be required to approve any Registration Form or other application to be a Participant.

ph.06-RR.01
4.2 Registration by Agreement. How Participants may enter into a written Registration Agreement with the SNO. A person may register with [SNO Name] as a Participant by entering into a written Registration Agreement with [SNO Name]. Such a Registration Agreement shall describe: (a) the Participant's Participant Type, as described in Section 4.3.2 (Participant Type); (b) whether the Participant is a Data Provider or a Data Recipient, or both; (c) if the Participant is registered as a Data Recipient, which of the Services the Participant may use; and (d) such other terms and conditions as [SNO Name] and the Participant shall agree.

ph.06-RR.01
1. Patient Access. [State Organization] hereby authorizes Patient to have access only to their own information contained in the Network and the Databases, for the following uses and purposes:

- Patient's own healthcare treatment.
- Payment of Patient's healthcare services.
- Auditing and monitoring compliance with the terms and conditions of this Agreement

ph.06-RR.01
[State Organization] is a health information exchange (HIE) organization formed for the purpose of facilitating the exchange of health information between and among providers, patients and authorized third-party entities. [State Organization] is not a Covered Entity within the definition of HIPAA (as defined below). The patient authorizes exchange of their personal information through participation in this agreement. As part of this activity, [State Organization] allows participating patients and providers access to personal health information held by other participating organizations through the [State Organization] Network (the "Network").

ph.06-RR.01
WHEREAS, Provider desires to obtain access to use the Network and, accordingly, has completed and executed the necessary portions of this Agreement, as well as reviewing and agreeing to the various policies of the Network.

ph.06-RR.01
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a

Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

ph.06-RR.01
4.3.1 Registration Form. How the SNO administers online registration. Each person wishing to register online to access the System and use the Services as a Participant shall complete the Registration Form provided by [SNO Name] at [insert web address]. [SNO Name] may change its Registration Form at any time. A person's Registration Form shall be that person's application to become a Participant.

ph.06-RR.01
4.3.4 Acceptance of Registration. How registration agreements will be created for online registrants. Upon [SNO Name]'s acceptance of a Registration Form, that Registration Form will be the Participant's Registration Agreement and shall be legally binding upon [SNO Name] and the Participant as of the effective date [SNO Name] shall provide to the Participant.

ph.06-RR.01
6. Data Recipient's Right to Use Services. Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services). Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data to the SNO) appear in Section 7 (Data Provider's Obligations). If the Participant is registered with [SNO Name] as a Data Recipient, the terms of this Section 6 (Data Recipient's Right to Use Services) shall apply to that Participant.

ph.06-RR.01
6.1 Grant of Rights. The nature of the Data Recipient's right to use the SNO's System and Services.

ph.06-RR.01
6.1.1 Grant by [SNO Name]. The SNO's grant of a license to use the SNO Services [SNO Name] grants to each Data Recipient, and each Data Recipient shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System and the Services for which that Data Recipient has registered, subject to the Data Recipient's full compliance with the Terms and Conditions and the Data Recipient's Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Recipient shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

ph.06-RR.01
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

ph.06-RR.01
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

ss.05-RR.01
The signatories recognize that, in order to safeguard the health of their populations and facilitate emergency preparedness and response, their respective agencies or ministries charged with the protection of public health should exchange individual and/or population-level or epidemiological health data, consistent with, all applicable laws in their respective jurisdictions.

RR.02 Acceptance of Compliance with other Policies/Procedures Adopted by the HIE (Current and Future)

ss.05-RR.02
Each signatory will endeavor to provide health data regarding an infectious disease agent or public health even to every signatory to which it is relevant. Exchange of data will occur according to the policies and procedures that are adopted by the working group and contained in the most recently approved "[Name] Health Initiative Infectious Disease Emergency Communications Guideline."

sp.08-RR.02
Any release of information outside the intended use of [IIS] is the responsibility of Clinic, and should be conducted in the same manner as any release of patient/client immunization histories. Clinic agrees to have written policy or procedures in place to ensure the security of immunization records. Use of information in an inappropriate manner is a Class 1 misdemeanor per SDCL 34-22-12.5.

ph.06-RR.02
Hospital shall abide by and follow the Exchange Policies and Procedures, attached hereto as Exhibit A, including but not limited to: enrollment of authorized users, user restrictions, audit trails, sanctions of users, privacy notices, restrictions on patient information, and response to patient requests.

sp.08-RR.02
All individuals who wish to participate as a user of the [Immunization] Registry must sign and comply with the [Immunization] Registry User Security and Confidentiality Agreement. Any use of the [Immunization] Registry that violates the [Immunization] Registry User Security and Confidentiality Agreement will subject the user to revocation of the user's access privileges and may result in civil or criminal penalties for improper disclosure of health information.

sp.08-RR.02
Staff of any health care entity or school who will be given access to the [Immunization] Registry must sign the [Immunization] Registry User Security and Confidentiality Agreement. The document contains details about the use of data contained in the [Immunization] Registry. [Immunization] Registry data is confidential. Breach of confidentiality requirements will subject the user, health care entity or school to termination from participation in the [Immunization] Registry and may result in civil or criminal penalties for improper disclosure of health information.

ph.06-RR.02
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

sp.02-RR.02
Policies and procedures for participation in [Program] and for the use, maintenance and operation of the [Program] Cardiac Registry are adopted and enforced by the [Program] Management Committee.

ph.06-RR.02
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

ph.06-RR.02
11.1 Compliance with Terms and Conditions. The SNO's obligations to require that all Participants agree to be bound by the SNO Terms and Conditions. [SNO Name] shall require that all Participants enter into a Registration Agreement or another legally binding agreement to comply with the Terms and Conditions in such form as [SNO Name] determines is appropriate.

ph.06-RR.02
All [Participants] must agree to the terms and conditions of [SNO Name]'s [Participant] Registration Agreement, which provides as follows:

1. [SNO Name] Terms and Conditions. All of the terms of the [SNO Name] Terms and Conditions are hereby incorporated by reference into this [Participant] Registration Agreement. Words in this [Participant] Registration Agreement shall have the meanings given to them by the [SNO Name] Terms and Conditions. All Applicants are required to read and agree to the [SNO Name] Terms and Conditions prior to completing this application.

ph.06-RR.02
6.3 Prohibited Uses. The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any. A Data Recipient shall not use or permit the use of the System or the Services for any prohibited use described in the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, a Data Recipient shall not use or permit the use of the Services for any use or purpose described below:]

ph.06-RR.02
9.1 Compliance with Policies and Procedures. Provisions requiring compliance with the Common Framework Policies and Procedures. [SNO Name] and each Participant shall comply with the standards for the confidentiality, security, and use of patient health

information, including without limitation protected health information described in HIPAA, as provided in the Common Framework Policies and Procedures, which is incorporated herein by reference. Each Participant shall comply with such standards regardless of whether or not that Participant is a "covered entity" under HIPAA.

9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security, and use laws imposed at the state and/or local level. [SNO Name] and each Participant shall comply with the requirements for the privacy, security, and use of patient health information imposed under the laws of the State of _______________. Without limiting the generality of the foregoing, [SNO Name] and each Participant shall comply with the following: [list of state or local legal requirements, if desired].

ph.06-RR.02
6.1.1 Grant by [SNO Name]. The SNO's grant of a license to use the SNO Services [SNO Name] grants to each Data Recipient, and each Data Recipient shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System and the Services for which that Data Recipient has registered, subject to the Data Recipient's full compliance with the Terms and Conditions and the Data Recipient's Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Recipient shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

ph.06-RR.02
6.1.2 Applicable Common Framework Policies and Procedures. The terms of the Common Framework Policies and Procedures that apply to a Data Recipient's right to use the SNO Services and ownership of the network and information obtained through the network. All issues concerning the ownership and rights in the NHIN and data and information obtained there from shall be as set forth in the Common Framework Policies and Procedures, which is incorporated herein by reference.

ph.06-RR.02
4.3.4 Acceptance of Registration. How registration agreements will be created for online registrants. Upon [SNO Name]'s acceptance of a Registration Form, that Registration Form will be the Participant's Registration Agreement and shall be legally binding upon [SNO Name] and the Participant as of the effective date [SNO Name] shall provide to the Participant.

ph.06-RR.02
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-RR.02
4.3.1 Registration Form. How the SNO administers online registration. Each person wishing to register online to access the System and use the Services as a Participant shall complete

the Registration Form provided by [SNO Name] at [insert web address]. [SNO Name] may change its Registration Form at any time. A person's Registration Form shall be that person's application to become a Participant.

ph.06-RR.02
4.4 Effect of Terms and Conditions Upon Registration Agreements. How Participants will agree to comply with the Terms and Conditions. Each Registration Agreement shall incorporate by reference, and require that the Participant agree to comply with, the Terms and Conditions. [SNO Name] may make exceptions to this Section 4.4 (Effect of Terms and Conditions Upon Registration Agreements), in [SNO Name]'s sole discretion, pursuant to any written Registration Agreement entered into as described in Section 4.2 (Registration by Agreement).

ph.06-RR.02
The Model assumes that the SNO Terms and Conditions will contain virtually all of the material terms and conditions that apply to a Participant's use of the SNO's System and Services, and therefore will contain most of the terms of each Participant's multilateral participation agreement. Under this approach, both written and online Registration Agreements will incorporate the SNO Terms and Conditions by reference and contain only those additional terms that apply to the Participant alone, e.g., the Participant's name, whether the Participant is a Data Provider or Data Recipient or both, the Participant's Participant Type, etc. The Model gives the SNO broad discretion to create exceptions to the Terms and Conditions, as the SNO determines necessary for particular Participants that enter into written Registration Agreements. The SNO should exercise care in making such exceptions, lest it undermine the effectiveness of the Terms and Conditions with respect to other Participants.

ph.06-RR.02
4.5 Changes to Terms and Conditions. How Participants will be aware of changes to the SNO Terms and Conditions, and will be legally obligated to comply therewith. [SNO Name] may amend, repeal and replace the Terms and Conditions at any time, and shall give Participants notice of those changes, as described in Section 3.2 (Development and Dissemination; Amendments). Subject to Section 4.6 (Termination Based on Objection to Change), any such change to the Terms and Conditions shall automatically be incorporated by reference into each Registration Agreement, and be legally binding upon [SNO Name] and the Participant, as of the effective date of the change.

ph.06-RR.02
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

ph.06-RR.02
WHEREAS, Provider desires to obtain access to use the Network and, accordingly, has completed and executed the necessary portions of this Agreement, as well as reviewing and agreeing to the various policies of the Network.

mm.06-RR.02
This policy applies to the following personnel: all persons who receive access to [Organization] through the Provider, including, but not limited to, medical records

personnel, information technology and support center personnel, medical staff, and employees involved in health care operations. This policy covers the minimum necessary standards for privacy and confidentiality. Providers who participate in [State Organization] may enact procedures that are more stringent than this policy, but must not allow those procedures to conflict with, or be less restrictive than this policy.

mm.06/(P2)-RR.02
Providers who participate in [Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [Organization] in accordance with such agreement.

ph.06-RR.02
B. Provider agrees to be bound by the restrictions and conditions of paragraphs A-K of Section III to the extent Provider has access to PHI of other Providers through [State Organization]. [State Organization] reserves the right to terminate Provider's access to the Network and access to the Databases at any time that [State Organization] has reason to believe that Provider has violated any of the conditions set forth in Section III or has accessed any information that Provider would not otherwise be authorized to receive pursuant to this Agreement.

ph.06-RR.02
Provider agrees to be bound by the policies and procedures of [State Organization], as may be amended from time to time by [State Organization]. The policies and procedures of [State Organization] shall be considered a part of this Agreement. Provider agrees to review these policies and procedures with employees and to obtain an attestation of such policies and procedures from each employee prior to providing access to the Network.

ph.06-RR.02
All of the terms of the [State Organization] Master Data Sharing Agreement - Terms and Conditions ("Terms and Conditions"), and the [State Organization] Policies and Procedures ("Policies and Procedures"), are hereby incorporated by reference into this Participant Registration Agreement. Words in this Participant Registration Agreement shall have the meanings given to them by the Terms and Conditions, and Policies and Procedures. Participant hereby represents and warrants that Participant, or an authorized person acting on Participant's behalf, has read and agrees to comply with the Terms and Conditions, and Policies and Procedures.

mm.07-RR.02
Providers who participate in [Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers may also be required to provide [Organization] with a list of active staff members with access to [Organization], in accordance with the Provider Participation Agreement. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [Organization] in accordance with such agreement.

b. Patient desires to obtain access personally and permit authorized users of their choice to use the Network and the information and databases supplied by all providers participating in the Network (the Databases") and, accordingly, has completed and executed the necessary portions of this Agreement, as well as reviewing and agreeing to the various policies of the Network.

ph.06-RR.02
Patient desires to obtain access personally and permit authorized users of their choice to use the Network and the information and databases supplied by all providers participating in the Network.

ph.06-RR.02
Alternative One: The SNO Terms and Conditions permit Participants to use the System and the Services for any use permitted by the Common Framework Policies and Procedures. A Data Recipient may use the System and the Services for which the Participant has registered only for the permitted purposes described in the Common Framework Policies and Procedures, which is incorporated herein by reference.

ph.06-RR.02
OR Alternative Two: The SNO Terms and Conditions would permit a narrower range of use than permitted by the Policies and Procedures, such as limiting use to the location and retrieval of specified data sets. A Data Recipient may use the System and the Services only to locate and retrieve the following data sets described for each Service as described on Schedule 6.2 (Permitted Uses).

RR.03 Scope of Use of Services Available to Recipient

ph.06-RR.03
OR Alternative Three: The SNO Terms and Conditions would permit specific uses for different types of Data Recipients, based on the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type). A Data Recipient may use the System and the Services only for the permitted uses described on Schedule 6.2 (Permitted Uses) that apply to the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type).

ph.06-RR.03
Hospital License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, the Hospital is hereby granted a limited license to allow its Authorized Users (as defined in Exhibit A) to remotely access and use the Exchange and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by Network. Any access to or use of the Exchange not expressly permitted in this Agreement is prohibited. Except as expressly permitted in this Agreement, Hospital shall not, and shall not allow or authorize any third party to: (i) use or access to the Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of the Exchange, or reverse engineer, disassemble, or decompile the Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use the Exchange, in whole or in part, to a third party. Hospital in no event shall access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation. Except as expressly set forth in this Agreement, Hospital will not obtain any rights in the Exchange, Documentation, any of the technology used to create the Exchange, including electronic formats and tools that Network or Access Provider uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by Network, Access Provider, or Host to develop, maintain, and operate the Exchange and deliver services to Hospital.

mm.10-RR.03
Connectivity to the XDS Affinity Domain from External Systems
Interoperability Strategy

The Policy Agreement shall identify the procedure for how to reach the data over the domain borders. There are many ways to bring this about and it is therefore very important that this is specified in the Agreement.

mm.10-RR.03
Organizational Rules

Describe the organizational rules for the XDS Affinity Domain. Detail the administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties.

hh.06-RR.03
a. Each enrolling Network must place appropriate restrictions on each Authorized User upon enrollment, as follows:

1. Hospitals and other Facilities. Facilities shall, prior to becoming Authorized Users, agree to access or input Data relating solely to patients.

2. Health Care Licensees. Physicians and other licensed providers may have access to any patient's information when they are the patient's primary, admitting, attending, consulting, or operating physician.

hh.06-RR.03
b. No exchange will allow any Authorized User access to any patient information from a dedicated acute in-patient or outpatient psychiatric unit or an in-patient or outpatient substance abuse facility, as designated by each Network.

hh.06-RR.03
c. If possible, each Network will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

hh.06-RR.03
d. Each Network will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network information system or Authorized User system, as applicable.

hh.06-RR.03
5.5 Purposes of Access. Authorized Users shall use the Exchange solely to access patient information in the following situations:

[a. Pursuant to the purposes specified in 45 C.F.R. §164.506(c) (the HIPAA regulations):

For treatment activities of any health care provider.

If the patient information was created at the covered entity for which the Authorized User works, for the payment or health care operations purposes of that covered entity.

If the patient information was not created at the covered entity for which the Authorized User works, for the payment activities of that covered entity, and for the health care operations activities of that covered entity, if that entity either has or had a relationship with the patient and the information is needed to conduct quality assessment and improvement activities or review the competence or qualifications of healthcare professionals.]

sp.06-RR.03

8. The parties mutually agree that the aforesaid file(s) (and/or any derivative file(s) [includes any file that maintains or continues identification of individuals]) may be retained by the User until _____, hereinafter known as the "retention date" The User agrees to notify CMS within 30 days of the completion of the purpose specified in section 6 if the purpose is completed before the aforementioned retention date. Upon such notice or retention date, whichever occurs sooner, CMS will notify the User either to return all data files to CMS at the User's expense or to destroy such data. If CMS elects to have the User destroy the data, the User agrees to certify the destruction of the files in writing within 30 days of receiving CMS=s instruction. A statement certifying this action must be sent to CMS. If CMS elects to have the data returned, the User agrees to return all files to CMS within 30 days of receiving notice to that effect. The User agrees that no data from CMS records, or any parts thereof, shall be retained when the aforementioned file(s) are returned or destroyed unless authorization in writing for the retention of such file(s) has been received from the appropriate Systems Manager or the person designated in item No. 22 of this Agreement. The User acknowledges that stringent adherence to the aforementioned retention date is required, and that the User shall ask CMS for instructions under this paragraph if instructions have not been received after 30 days after the retention date.

sp.06-RR.03

The User agrees to submit to CMS a copy of all findings within 30 days of making such findings. The parties mutually agree that the User has made findings with respect to the data covered by this Agreement when the User prepares any report or other writing for submission to any third party (including but not limited to any manuscript to be submitted for publication) concerning any purpose specified in section 6 (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the files specified in section 7 or any data derived from such files). The User agrees not to submit such findings to any third party until receiving CMSUs approval to do so. CMS agrees to make determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individual beneficiaries could not be identified. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries. The User agrees further to submit its findings to the National Technical Information Service (NTIS, 5285 Port Royal Road, Springfield, Virginia 22161) within 30 days of receiving notice from CMS to do so.

sp.06-RR.03

The User understands and agrees that they may not reuse original or derivative data file(s) without prior written approval from the appropriate System Manager or the person designated in section 22 of this Agreement.

ph.06-RR.03

The Model assumes that the Common Framework Policies and Procedures will describe generally the scope of permitted uses of the Network and information Data Recipients will be able to access through the Network. The Model provides that Data Recipients may use only those services for which the Data Recipient has registered pursuant to Section 4.1 (Registration Required). The SNO Terms and Conditions may also permit a variety of additional uses, so long as they are not prohibited by the Common Framework Policies and Procedures, e.g., aggregating data for research and chronic disease management studies, public health functions, and measuring provider compliance with standards and protocols such as pay-for-performance standards.

ph.06-RR.03
OR Alternative Two: The SNO Terms and Conditions would permit a narrower range of use than permitted by the Policies and Procedures, such as limiting use to the location and retrieval of specified data sets. A Data Recipient may use the System and the Services only to locate and retrieve the following data sets described for each Service as described on Schedule 6.2 (Permitted Uses).

ph.06-RR.03
Alternative One: The SNO Terms and Conditions permit Participants to use the System and the Services for any use permitted by the Common Framework Policies and Procedures. A Data Recipient may use the System and the Services for which the Participant has registered only for the permitted purposes described in the Common Framework Policies and Procedures, which is incorporated herein by reference.

ph.06-RR.03
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

ph.06-RR.03
The Model assumes that the Participant will be permitted to select its Authorized Users without review or approval by the SNO. The SNO may, however, wish to adopt specific credentialing criteria for Authorized Users that would be administered by the SNO, and which may, if desired, be set forth in the SNO Terms and Conditions. The Model assumes that Participants will be required to inform the SNO of changes to their lists of Authorized Users on an ongoing basis. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users.

pp.06-RR.03
If Business Associate is requested to make a disclosure for one of the foregoing reasons, it shall forward such request to the Covered Entity so that the Covered Entity can coordinate and prepare a timely response. Business Associate shall make PHI available to the Covered Entity for the foregoing reasons if requested to do so in writing by the Covered Entity for the Covered Entity to coordinate and prepare a timely response.

Notwithstanding Section 8.01(a), Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Furthermore, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

ph.06-RR.03
Participant is a Hospital Type within the meaning of Section 4.3.2 of the Terms and Conditions. Participant shall be both a Data Provider and a Data Recipient, as such terms are used, and with such rights and obligations, as are set forth in the Terms and Conditions

and the Policies and Procedures. [During the Initial Registration Period, Participant shall have the right to only such Services as [Organization] may, in its sole discretion, make available. Participant agrees to be bound by, and to comply with, all of the provisions of the Terms and Conditions, and Policies and Procedures, and expresses such agreement by affixing its signature to this Registration Agreement. Accordingly, Participant may commence to access and use [Organization]'s System and Services, subject to all of the provisions of this Registration Agreement, the Terms and Conditions, and Policies and Procedures.]

sp.07-RR.03
ss.07-RR.03
The facility will provide its staff member's access to computer equipment and electronic communications necessary to operate the [State] SIIS. The facility agrees to enter client demographic and immunization information into the [State] SIIS in a timely manner for those receiving immunizations at the facility.

sp.07-RR.03
ss.07-RR.03
Access to this system is granted only for the purposes of recording and/or verifying immunization requirements. This information is to be shared on an as needed basis only with school officials, public health officials, child day care centers, other health care professionals or health institutions, the person's legal guardian, or other institutions required by law to collect immunization records.

ss.07-RR.03
Access to this system is granted only for the purposes of verifying or assessing the immunization status or need of individuals.

sp.07-RR.03
ss.07-RR.03
This information is to be shared on an as needed basis only with school officials, public health officials, child day care centers, other health care professionals or health institutions, or other institutions required by law to collect immunization records.

pp.06-RR.03
If a Business Associate provides data aggregation services, the Business Associate may use PHI to provide data aggregation services to a Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B), except as otherwise provided by this Agreement.

pp.06-RR.03
Section 12.02 Use and Disclosure of Information After Termination. Upon the complete termination of this Agreement, the Participants agree that the Information stored on the Network as of the date of the termination of the Agreement shall remain on the Network for use and disclosure, subject to [Organization]'s desire to continue maintaining the Network, under the following conditions:

purposes, including, but not limited to, publication of research results in accordance with ARTICLE VII and ARTICLE VIII. After the two-year period, Participants may request that their Information no longer be used or disclosed for any purpose. Until such a request is made, [Organization] may continue to use the Information in compliance with this Section, provided [Organization] gives prior written notice to the affected Participants of any such use. Notwithstanding the foregoing, Information must continue to be stored on the Network for a longer period of time to the extent that Participants have agreed to make their

Information available for research project approved pursuant to ARTICLE VII, in which case the Information shall continued to be stored, and may continue to be used and disclosed, for the duration of such research projects in compliance with the terms of the projects. After the applicable period discussed above, [Organization] shall no longer use or disclose the Information for research purposes and the provisions of ARTICLE V (Confidentiality) and ARTICLE VIII (HIPAA Business Associate Provisions) shall continue to apply to the Information.

pp.06-RR.03
Section 7.04 Guidelines for Using and Disclosing Information. When a research project has been approved pursuant to Section 7.02 or Section 7.03, [Organization] shall act as the Participants' Business Associate for purposes of disclosing the Information to the researchers. [Organization] shall use the following guidelines when using or disclosing PHI or deidentified data:

Initial Determination of Scope of Information To Be Disclosed. For each research project, [Organization] shall make a threshold determination of whether the minimum necessary use or disclosure of Information to comply with the request involves the use or disclosure of identifiable Information, a Limited Data Set, or deidentified Information. In making this threshold determination and when further disclosing Information in connection with the research project, [Organization] may rely on and adopt the determination of an Institutional Review Board as to the scope of the minimum necessary disclosure for the research project. If a research disclosure is made pursuant to an Individual's authorization, the scope of the authorization shall constitute the minimum necessary disclosure. In the event [Organization] determines it is necessary to disclose the entire subset of Information on the Network concerning an Individual to comply with the research request, [Organization] will document the justification for releasing the entire subset of Information. An Institutional Review Board's determination that the entire subset of Information on the Network is necessary, or an Individual's authorization, shall constitute such documentation.

Conditions For Disclosing Individually Identifiable Health Information. If PHI is requested for a research project, [Organization] shall not use or disclose the PHI unless: (A) authorizations that comply with the Privacy Rule allowing the use or disclosure of the PHI for the specific research purpose are obtained or have obtained from all Individuals whose PHI will be used or disclosed; or (B) a waiver of the authorization is obtained from an appropriate Institutional Review Board or Privacy Board in accordance with 45 CFR § 164.512(i). Notwithstanding the foregoing, [Organization] may use or disclose identifiable PHI for reviews preparatory to research (consistent with 45 CFR § 164.512(i)(1)(ii)) and for research on decedent's information (consistent with 45 CFR § 164.512 (i)(1)(iii)) without an authorization or the waiver thereof; provided that the use or disclosure of the PHI is consistent with the minimum necessary standard of the Privacy Rule. This Section 7.04(b) shall not apply to information in a Limited Data Set or deidentified information.

Conditions For Disclosing Limited Data Sets. If a Limited Data Set is requested for a research project, [Organization] shall not use or disclose the Information unless [Organization], on behalf of the affected Covered Entity Participants, obtains a "Data Use Agreement" from the individual or entity using the Limited Data Set or to which the Limited Data Set will be disclosed. Such Data Use Agreement shall comply with the requirements of 45 CFR § 164.514(e). [Organization] further agrees to maintain copies of all Data Use Agreements related to Covered Entity Participants' Information and to forward same to the Covered Entity upon request.

Conditions For Disclosing Deidentified Information. If deidentified Information is used or disclosed, [Organization] shall act as Covered Entities' Business Associate for purposes of deidentifying the Information and shall ensure that no health information that is used or disclosed identifies an Individual and that there is no reasonable basis to believe that the information can be used to identify an Individual. All deidentification of PHI shall be conducted in compliance with 45 CFR § 164.514(a) – (c).

pp.06-RR.03
Section 8.05 Access to Records. Business Associate shall provide reasonable access to PHI in a Designated Record Set in the Business Associate’s possession to the Covered Entity to which the PHI belongs in order for the Covered Entity to meet the requirements under 45 CFR § 164.524 with regard to providing an Individual with a right to access the Individual’s PHI. Prior to making a request to Business Associate under this Section, Participants shall make a good faith effort to gather the requested PHI from their own data sources that feed the Network. In any event, Business Associate shall not respond directly to requests from Individuals for access to their PHI in a Designated Record Set. Business Associate will refer such Individuals to the relevant Covered Entity so that the Covered Entity can coordinate and prepare a timely response to the Individual.

pp.06-RR.03
Upon a Participant’s withdrawal, the Information stored by such Participant on the Network shall no longer be accessible by the Full Participants and all confidentiality provisions contained in this Agreement shall remain in force. Notwithstanding, Information may continue to be used and disclosed for the reasons described in Section 12.05.

ph.02-RR.03
c. RESEARCHER may use or disclose data subject to this Agreement and included in limited data sets obtained from PROVIDER/REPOSITORY, solely for purposes of research testing the functioning of the BIOSURVEILLANCE systems.

ph.02-RR.03
9. No Identification of or Contact with Individuals. Data subject to this Agreement shall not be used to identify or to contact any individual who is a subject of the data.

pp.05-RR.03
The Entity acknowledges that this Agreement does not give the Entity any rights with respect to the information which is available to Providers under their Individual Provider Information Sharing Agreements. The disclosure of all such information to the Provider is subject to [Entity]’s and the Providers’ Joint Obligations to Maintain Patient Privacy under that Agreement.

ph.06-RR.03
1. Patient Access. [State Organization] hereby authorizes Patient to have access only to their own information contained in the Network and the Databases, for the following uses and purposes:

- Patient’s own healthcare treatment.
- Payment of Patient’s healthcare services.
- Auditing and monitoring compliance with the terms and conditions of this Agreement.

ph.06-RR.03
Authorized Users. Terms that govern use of the services by the Participant’s Authorized Users. The Model assumes that user agreements will not be required of every individual who uses the SNO’s System or Services. Instead, Participants will be responsible for designating

the individuals within their organizations who would be authorized to use the SNO's System and Services ("Authorized Users").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will access the SNO's System and/or use the SNO's Services. Each Participant shall provide [SNO Name] with a list in a medium and format approved by [SNO Name] identifying all the Participant's Authorized Users, together with the information described in Schedule 5 (Required Information for Authorized Users), to enable [SNO Name] to establish a unique identifier for each Authorized User. The Participant shall update such list whenever an Authorized User is added or removed by reason of termination of employment or otherwise.

ph.06-RR.03
5.2 Certification of Authorized Users. How the Participant will provide assurances that its Authorized Users have been trained appropriately. At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User: (a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training); (b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type); (c) Has agreed not to disclose to any other person any passwords [and/or other security measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms); (d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and (e) [Others, if desired].

ph.05-RR.03
User, and any Authorized Party on User's behalf, may use the Limited Data Set only for the following purposes:

ss.05-RR.03
Health data will be maintained and kept by receiving signatories according to the law by which the receiving signatories are bound and for the reason intended by the sending jurisdiction.

hh.06-RR.03
[Authorized Users shall use such Data solely for purposes of payment, treatment and healthcare operations as each of those terms is defined in the HIPAA Regulations.]

sp.08-RR.03
The [Immunization] Registry Disclosure Form provided by the [Name], Immunization Program, or available from the [Immunization] Registry website, includes notification that data from the immunization encounter may be recorded in the [Immunization] Registry for sharing among participating immunization providers. The parent, guardian or legal custodian may choose to refuse to participate in the [Immunization] Registry, thus preventing [Immunization] Registry users from accessing their child's immunization information.

sp.08-RR.03
The parent, guardian or legal custodian may have the patient's record excluded from the Registry by completing the [Immunization] Registry Refusal to Share Request Form and submitting the completed form to the [Immunization] Registry. The [Immunization]

Registry database administrator will then update the child record to indicate that data is not to be shared. If a [Immunization] Registry provider subsequently tries to access that patient record, the provider will be unable to view the patient's immunization history and personal information. Only [Immunization] Registry staff has the ability to view or unlock a locked record. If an electronic data transfer includes data on a child who has been excluded, the child's data will not be transferred to the [Immunization] Registry.

sp.08-RR.03
The information contained in the [Immunization] Registry shall only be used for the following purposes:

- To provide immunization services to the patient parent, guardian or legal custodian, including reminder/recall notices.
- Permit schools to determine the individual immunization status of their students.
- Provide or facilitate third party payments for immunizations, (e.g., medical assistance, HMOs).
- Compile and disseminate non-identifying, statistical information of immunization status on groups of children or populations in [City].
- Assist providers in keeping a child's immunization status up-to-date including historical validations and real-time recommendations based on a pre-determined schedule.
- Prevent the administration of duplicate immunizations.

sp.08-RR.03
Clinic is responsible for appropriately using the [IIS] software for the sole purpose of participating in [IIS]. The [IIS] purpose is to maintain a database of all children immunized at Clinic and in [State] with a goal of age-appropriate immunizations. Other uses of [IIS] are inappropriate and forbidden. Inappropriate uses of the software include, but are not limited to, assisting in bill collection or locating or identifying persons for reasons other than increasing immunization levels. Inappropriate uses may result in Clinic's exclusion from the [IIS], as well as other civil or criminal penalties.

RR.04 Prohibitions on Recipient's Use of Data

sp.08-RR.04
Clinic is responsible for appropriately using the [IIS] software for the sole purpose of participating in [IIS]. The [IIS] purpose is to maintain a database of all children immunized at Clinic and in [State] with a goal of age-appropriate immunizations. Other uses of [IIS] are inappropriate and forbidden. Inappropriate uses of the software include, but are not limited to, assisting in bill collection or locating or identifying persons for reasons other than increasing immunization levels. Inappropriate uses may result in Clinic's exclusion from the [IIS], as well as other civil or criminal penalties.

sp.08-RR.04
Identifying information contained in the [Immunization] Registry will only be accessible to [City] Department of Public Health personnel, their authorized agents and authorized users. Requests for data for research purposes that go beyond the scope of the individual provider's patients or the local health department area of jurisdiction must be forwarded to the [Immunization] Registry Coordinator.

mm.06-RR.04
C. Response to Patient Requests

1. When responding to requests for release of patient information, Network member hospitals shall not release data accessed or obtained through Exchange. Each hospital shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient's medical record and the system does not maintain patient data. Exchange simply queries and collates patient data from the participating providers.

mm.06-RR.04
Each enrolling hospital must place appropriate restrictions on each Authorized User upon enrollment, as follows:

Exchange Physicians. Physicians with staff privileges at a Exchange hospital may have access to any patient's information when they are identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. If an Exchange physician wants access to other patients' information, a message will appear stating: "Our records indicate that you do not have an existing relationship with the patient you have selected. To continue, you agree that you need this information for the continuing care and treatment of the patient. Your access to this information is subject to audit and review." To access that patient's information, the Exchange physician must click on the "Continue" button and the override will be recorded in the audit trail.

mm.06-RR.04
Exchange Physician Office Staff. These individuals may have access to any patient's information only when a physician associated with that office is identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. These individuals have no override privileges to view other patients' information. However, a Network member hospital may allow at least one key member of each physician's office staff to have override privileges to view other patients' information, subject to the same audit and review process as the physicians' override privileges.

mm.06-RR.04
Exchange ED Physicians and ED Clinicians. These individuals may have access to all patient information and may access any patient information when such information is needed for the patient's continuing care and treatment, subject to the same audit and review process. Each Exchange hospital's ED clinical director or hospital clinical director shall determine which ED RNs shall have access privileges.

mm.06-RR.04
Exchange Health Care Providers. These individuals may have access only to patient information at the Exchange hospital that enrolled the user and cannot access patient information from other Exchange hospitals. These users may only view a patient's information if the enrolling hospital has created a link between the user and the patient to establish a relationship. These individuals have no override privileges to view other patients' information. These users may not search for patients at other Exchange hospitals.

mm.06-RR.04
Exchange Hospital Case Managers. These individuals may have access to any patient's information when the user is serving as a case manager for the patient and the information is needed for the continuing care and treatment of the patient. The Exchange hospital desiring to provide access to the user must establish a link between the user and a patient. These individuals have no override privileges to view other patients' information.

mm.06-RR.04
Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient's data through Exchange. If a patient has chosen this option, when a query is made about that particular patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details." If a patient desires to revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

mm.06-RR.04
Authorized Users shall use the Exchange solely to access patient information in the following situations:

a. Pursuant to the purposes specified in 45 C.F.R. §164.506(c) (the HIPAA regulations):

For treatment activities of any health care provider.

If the patient information was created at the covered entity for which the Authorized User works, for the payment or health care operations purposes of that covered entity.

If the patient information was not created at the covered entity for which the Authorized User works, for the payment activities of that covered entity, and for the health care operations activities of that covered entity, if that entity either has or had a relationship with the patient and the information is needed to conduct quality assessment and improvement activities or review the competence or qualifications of healthcare professionals.

b. Pursuant to a valid authorization when required by 45 C.F.R. §164.508 or 42 C.F.R. § 2.1, et seq., or pursuant to a valid authorization or consent when required by [State] law.

ph.06-RR.04
Hospital shall be responsible for ensuring the security and confidentiality of the password protected accounts within the Exchange to which Hospital's employees are granted access in order to access and use the Exchange ("Data User Account"), including, without limitation, all user IDs and passwords assigned to such Data User Accounts. Hospital employees shall not disclose their Data User Accounts to any third party, and Hospital employees hereby are expressly prohibited from sharing their Data User Accounts with any third party.

sp.08-RR.04
[Immunization] Registry data identifying children will not be disclosed to unauthorized individuals, including law enforcement, without the approval of the Director of the Division of Disease Control. All subpoenas, court orders, and other legal demands for [Immunization] Registry data received by any authorized user of the [Immunization] Registry must be brought to the attention of the [Immunization] Registry Coordinator, who will consult [Immunization Program Name] legal counsel.

sp.08-RR.04
Any non-health use of [Immunization] Registry data is prohibited and no user shall attempt to copy the database or software used to access the [Immunization] Registry.

sp.08-RR.04
The parent, guardian or legal custodian may have the patient's record excluded from the Registry by completing the [Immunization] Registry Refusal to Share Request Form and submitting the completed form to the [Immunization] Registry. The [Immunization] Registry database administrator will then update the child record to indicate that data is not to be shared. If a [Immunization] Registry provider subsequently tries to access that patient record, the provider will be unable to view the patient's immunization history and personal information. Only [Immunization] Registry staff has the ability to view or unlock a locked record. If an electronic data transfer includes data on a child who has been excluded, the child's data will not be transferred to the [Immunization] Registry.

sp.08-RR.04
The [Immunization] Registry Disclosure Form provided by the [IMMUNIZATION PROGRAM NAME], Immunization Program, or available from the [Immunization] Registry website, includes notification that data from the immunization encounter may be recorded in the [Immunization] Registry for sharing among participating immunization providers. The parent, guardian or legal custodian may choose to refuse to participate in the [Immunization] Registry, thus preventing [Immunization] Registry users from accessing their child's immunization information.

hh.06-RR.04
Any access to or use of the Exchange not expressly permitted in this Agreement is prohibited. Except as expressly permitted in this Agreement, neither Network shall, nor allow or authorize any third party to: (i) use or access an Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of an Exchange, or reverse engineer, disassemble, or decompile an Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use an Exchange, in whole or in part, to a third party.

sp.02-RR.04
b. [Entity] and the [Program] Management Committee will not disclose information from the [Program] Cardiac Registry that is identified by Participant and/or their associated Providers without authorization by the Participant.

sp.02-RR.04
c. In addition to the statutory CQIP protections, the following procedures shall be used to protect against the disclosure of information pertaining to Participants and their associated Providers:

(i). No information which allows the identification of a Participant or Participant's associated Individual Providers (if applicable), or is reasonably believed by the [Program] Management Committee to allow the linking of information concerning any case(s) or outcome(s) to any Participant or Participant's associated Individual Providers (if applicable) shall be disclosed without the written consent of the Participant, except in the event that such disclosure is required by court order.
(ii) In the event of a court order requiring such disclosure the [Program] Management Committee shall object to making the disclosure and, unless prohibited by law, shall give the Participant prompt notice and an opportunity to defend against the order.
(iii) In addition to the patient-identifiable information required to be excluded from Limited Data Sets, Participant- and Provider-identifiable information subject to Subsection 3(c)(i) shall be excluded from any Limited Data Set prepared under this Agreement unless otherwise authorized by the Participant.

(iv) The provisions of this Subsection shall survive the termination of this Agreement for any reason.

sp.02-RR.04
b. The Participant may use information received from the [Program] Cardiac Registry for planning, quality assessment and improvement, and related functions, and for research, provided that in the event the Participant is provided with Limited Data Sets or information derived from Limited Data Sets which include Protected Health Information provided by other [Program] Participants, the Participant will receive the information subject to the following conditions:

(i) The Participant shall use the information only for purposes of planning, quality assessment and improvement, or related functions, or as otherwise required by law;
(ii) Only the Participant and its associated Providers may receive or use the information;
(iii) The Participant will not use the information for any purpose other than those specified in Subsection 6(b)(i);

ph.05-RR.04
Not to use the information contained in the Limited Data Set to identify the individuals whose information is contained in the Limited Data Set, nor to contact them under any circumstances.

sp.06-RR.04
The User represents further that, except as specified in an Attachment to this Agreement or except as CMS shall authorize in writing, the User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person. The User agrees that, within the User organization, access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this section and to those individuals on a need-to-know basis only.

ph.06-RR.04
OR Alternative Three: The SNO Terms and Conditions would permit specific uses for different types of Data Recipients, based on the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type). A Data Recipient may use the System and the Services only for the permitted uses described on Schedule 6.2 (Permitted Uses) that apply to the Participant Type under which the Data Recipient is registered pursuant to Section 4.3.2 (Participant Type).

ph.06-RR.04
OR Alternative Two: The SNO Terms and Conditions would permit a narrower range of use than permitted by the Policies and Procedures, such as limiting use to the location and retrieval of specified data sets. A Data Recipient may use the System and the Services only to locate and retrieve the following data sets described for each Service as described on Schedule 6.2 (Permitted Uses).

ph.06-RR.04
5.4 No Use by Other than Authorized Users. A requirement that the SNO's System and Services be accessed and used only by Authorized Users. The Participant shall restrict access to the System and, if applicable, use of the Services, only to the Authorized Users the Participant has identified to [SNO Name] in accordance with Section 5.1 (Identification of Authorized Users).

ph.06-RR.04

5.2 Certification of Authorized Users. How the Participant will provide assurances that its Authorized Users have been trained appropriately. At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User: (a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training); (b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type); (c) Has agreed not to disclose to any other person any passwords [and/or other security measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms); (d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and (e) [Others, if desired].

ph.06-RR.04

Authorized Users. Terms that govern use of the services by the Participant's Authorized Users. The Model assumes that user agreements will not be required of every individual who uses the SNO's System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO's System and Services ("Authorized Users").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will access the SNO's System and/or use the SNO's Services. Each Participant shall provide [SNO Name] with a list in a medium and format approved by [SNO Name] identifying all the Participant's Authorized Users, together with the information described in Schedule 5 (Required Information for Authorized Users), to enable [SNO Name] to establish a unique identifier for each Authorized User. The Participant shall update such list whenever an Authorized User is added or removed by reason of termination of employment or otherwise.

ph.09-RR.04

5. Authorized Users. Terms that govern use of the SNO Services by the Participant's Authorized Users. The Model assumes that "user agreements" will not be required of every individual who uses the SNO's System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO's System and Services ("Authorized User").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will use the SNO's Services.

5.2 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users.

5.3 No Use by Other than Authorized Users. A requirement that the SNO's System and Services be accessed and used only by Authorized Users.

5.4 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users.

6. Data Recipient's Right to Use Services. Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services). Provisions that apply

specifically to "Data Providers" (i.e., Participants registered to provide data to the SNO) appear at Section 7 (Data Provider's Obligations).

6.1 Grant of Rights. The nature of the Participant's right to use the System and Services.

6.1.1. Grant by SNO. The rights granted by the SNO.

6.1.2. NHIN. The rights granted by the NHIN.

6.2 Permitted Uses. The permitted uses of the SNO's System and Services.

6.3 Prohibited Uses. The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any.

7. Data Provider's Obligations. Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data). Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services) appear at Section 6 (Data Recipient's Right to Use Services).

7.1 Grant of Rights. The nature of the Data Provider's right to use the System.

7.2 Provision of Data. Terms that apply to the Data Provider's delivery of data to the Network, e.g., format, standards, etc.

7.3 Measures to Assure Accuracy of Data. The Data Provider's obligations to provide accurate, complete, and timely information.

7.4 License. The Data Provider's agreement that the data it provides will be available for use through the Network.

ph.06-RR.04
1. Patient Access. [State Organization] hereby authorizes Patient to have access only to their own information contained in the Network and the Databases, for the following uses and purposes:

- Patient's own healthcare treatment.
- Payment of Patient's healthcare services.
- Auditing and monitoring compliance with the terms and conditions of this Agreement

ph.06-RR.04
[State Organization] hereby authorizes Provider to have access to the Network and the Databases accessible through the Network for the following uses and purposes:

A. Treatment of a patient of or by Provider.

ph.06-RR.04
Limitations on Patient Access. Patient access to certain information may be limited based on a provider's determination that such information may endanger the Patient or other identifiable persons. Patient can obtain the name of the provider limiting such access, and may appeal such denial of access with provider in accordance with provider's appeal procedures.

pp.05-RR.04
2. The Provider shall disclose information received from other providers through [Entity]'s information system about identified individual patients only to those individuals, to their parents or other legal guardians, to the Provider's employees, contractors, agents or other affiliates authorized to act on behalf of the Provider under this Agreement, or through [Entity] to other health care providers who have entered into an Health Care Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that patient, unless (a) the Provider obtains a release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-RR.04
8. The Provider shall obtain information about individual patients from [Entity] only for the purpose of providing health care to those patients and/or to utilize the information services which are identified in Appendix A (“Information Services”). In the event the Provider receives information indicating that any person associated with the Provider may have accessed information for any other purpose, the Provider shall notify [Entity] at once, and such person shall be denied further access pending [Entity]’s investigation. [Entity] may at its discretion deny access to any person [Entity] has reason to believe accessed information from [Entity] for a purpose other than those within the scope of this Agreement.

pp.05-RR.04
i) The Provider shall disclose information received from other providers through [Entity]’s information system about individual patients only to those patients, their parents or other legal guardians, or other health care providers who have entered into an Individual Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that patient, unless (a) the Provider obtains a release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-RR.04
8. The Provider shall obtain information about individual patients from [Entity] only for the purpose of providing health care to those patients and/or to utilize the information services which are identified in Appendix A (“Information Services”). In the event the Provider receives information indicating that any person associated with the Provider may have accessed information for any other purpose, the Provider shall notify [Entity] at once, and such person shall be denied further access pending [Entity]’s investigation. [Entity] may at its discretion deny access to any person [Entity] has reason to believe accessed information from [Entity] for an improper purpose.

pp.05-RR.04
2. The Insurer shall disclose information received through the Information System about identified Enrollees only to those individual Enrollees, to their parents or other legal guardians, or to the Insurer's employees, contractors, officers or agents authorized to act on behalf of the Insurer under this Agreement, or to Providers who have entered into an Health Care Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that Enrollee, unless (a) the Insurer obtains a Release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-RR.04
8. Any Immunization Data the Insurer obtains about identified Enrollees from [Entity] may only be used by the Insurer for purposes permitted by the Releases applicable to such Enrollees. In the event the Insurer receives information indicating that any person

associated with the Insurer may have accessed information for any other purpose, the Insurer shall notify [Entity] at once.

ph.02-RR.04
d. No other uses or disclosures are permitted under this Agreement unless expressly required by warrant, court order, subpoena or other demand or process by a court or agency of competent jurisdiction; provided that no such disclosure shall be made without prior notice to the Data Provider unless such notice is prohibited by law.

pp.06-RR.04
Upon a Participant’s withdrawal, the Information stored by such Participant on the Network shall no longer be accessible by the Full Participants and all confidentiality provisions contained in this Agreement shall remain in force. Notwithstanding, Information may continue to be used and disclosed for the reasons described in Section 12.05.

ph.02-RR.04
b. The Data Provider may require the omission of the following data elements from the limited data sets permitted under this Agreement, by designation upon entry into this Agreement as provided below: Provider Site Identifier, Encounter Site Identifier, Attending Physician Identifier.

mm.10-RR.04
Health data may be exchanged pursuant to the provisions of this Annex only for the purpose of preventing, detecting or responding to public health emergencies.

When health data is to be disseminated

sp.09-RR.04
- Expectations for sharing unpublished data (varies depending on data type)
- Recommendations regarding incentives for sharing unpublished data

sp.07-RR.04
I agree that no records will be accessed except for those records the [State] Department of Health’s Programs are requesting to be reviewed. The [State] Department of Health will periodically monitor the user’s activities related to the usage of [Immunization] registry.

pp.06-RR.04
Section 8.10 No Request to Use or Disclose in Impermissible Manner. Except as necessary for the management and administrative activities of the a Business Associate as allowed in Section 8.01(c), a Covered Entity shall not request a Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. No Business Associate shall be responsible for any compliance with, or failure to comply with, a request from Covered Entity to use or disclose PHI in a manner that would not be permissible under the Privacy Rule if done by Covered Entity.

pp.06-RR.04
In no event will [Organization] allow Information to be disclosed for research projects that have the effect of comparing the Participants (such as individual Participant outcomes, Participant financial information, or charges to patients or third-party payors and similar reimbursement data) without specific approval from each of the institutions involved or unless such comparisons are an implicit component of a research project that complies with the provisions of Section 7.02 or Section 7.03(a).

pp.06-RR.04
Section 7.06 Access to Network by Researchers. No researcher, other than [Organization], shall have direct access to identified Information on the Network (although access to deidentified Information and Limited Data Sets may be permitted if allowed under Section 7.02 or Section 7.03). Information that is not deidentified and that is requested by researchers other than [Organization] shall be retrieved by representatives of [Organization]. Any use of the Information for research by [Organization] shall be limited to the purpose of the research as approved or allowed by Section 7.02 or Section 7.03.

pp.06-RR.04
Section 8.01 Limits on Use and Disclosure.

Business Associate agrees to not use or further disclose PHI other than as permitted or required by this Agreement or as Required By Law. Business Associate may use and disclose PHI to perform those functions, activities, or services that Business Associate performs for, or on behalf of, each Covered Entity as specified in this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by a Covered Entity, including but not limited to storing Participant Information on the Network and maintaining the Network, making disclosures to Participants for Treatment purposes, using and disclosing Information for research purposes in compliance with ARTICLE VII, and reporting Information to appropriate governmental agencies for public health purposes (including, including, but not limited to, screening laboratory data on behalf of Covered Entities and making legally required reports to the [State] State Department of Health). Any such use or disclosure shall be limited to those reasons and those individuals as necessary to meet the Business Associate's obligations under this Agreement.

pp.06-RR.04
Notwithstanding the foregoing Section 12.04(a), if a Participant withdraws because of a significant breach of [Organization]'s duties under ARTICLE VII or ARTICLE VIII with regard to Information stored on the Network by the withdrawing Participant, the provisions of Section 12.04(a) shall not apply and [Organization] may no longer use or disclose the Information for research purposes.

pp.06-RR.04
Business Associate will not make the following disclosures that are otherwise allowed to be made by a Covered Entity under 45 C.F.R. § 164.512 unless compelled to do so by law or unless such a disclosure is specifically authorized or required by this Agreement (including, but not limited to, ARTICLE VII):

About victims of abuse, neglect, or domestic violence:

- For health oversight activities;
- For judicial and administrative proceedings;
- For law enforcement purposes.

About decedents:

- For cadaveric organ, eye, or tissue donation purposes;
- To avert a serious threat to health or safety;
- For specialized government functions;
- For workers' compensation purposes;
- For marketing purposes;
- For fundraising purposes.

ph.06-RR.04
1. [State Organization] may use and disclose PHI if necessary for proper management and administration of [State Organization] or to carry out the legal responsibilities of [State Organization].

ph.06-RR.04
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-RR.04
6.3 Prohibited Uses. The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any. A Data Recipient shall not use or permit the use of the System or the Services for any prohibited use described in the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, a Data Recipient shall not use or permit the use of the Services for any use or purpose described below:]

ph.06-RR.04
6.3.1. No Services to Third Parties. The Data Recipient shall use the System and the Services for which the Data Recipient has registered only for the Data Recipient's own account, and shall not use any part of the System or the Services to provide separate services or sublicenses to any third party, including without limitation providing any service bureau services or equivalent services to a third party.

ph.06-RR.04
6.3.2. No Services Prohibited by Local Laws. The Data Recipient shall not use the System or the Services for which the Data Recipient has registered for any purpose or in any manner that is prohibited by the laws of the State of ____________. Without limiting the generality of the foregoing, the Data Recipient shall comply with the following: [list of state or local legal requirements, if desired].

ph.06-RR.04
6.3.3. No Use for Comparative Studies. A Data Recipient shall not use the Services to aggregate data to compare the performance of other Participants and/or Authorized Users, without the express written consent of [SNO Name] and each of the Participants and Authorized Users being compared.

ph.06-RR.04;
Hospital License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, the Hospital is hereby granted a limited license to allow its Authorized Users (as defined in Exhibit A) to remotely access and use the Exchange and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by Network. Any access to or use of the Exchange not expressly permitted in this

Agreement is prohibited. Except as expressly permitted in this Agreement, Hospital shall not, and shall not allow or authorize any third party to: (i) use or access to the Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of the Exchange, or reverse engineer, disassemble, or decompile the Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use the Exchange, in whole or in part, to a third party. Hospital in no event shall access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation. Except as expressly set forth in this Agreement, Hospital will not obtain any rights in the Exchange, Documentation, any of the technology used to create the Exchange, including electronic formats and tools that Network or Access Provider uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by Network, Access Provider, or Host to develop, maintain, and operate the Exchange and deliver services to Hospital.

RR.05 Ensuring Compliance with Applicable Laws

ph.06-RR.05
Hospital License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, the Hospital is hereby granted a limited license to allow its Authorized Users (as defined in Exhibit A) to remotely access and use the Exchange and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by Network. Any access to or use of the Exchange not expressly permitted in this Agreement is prohibited. Except as expressly permitted in this Agreement, Hospital shall not, and shall not allow or authorize any third party to: (i) use or access to the Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of the Exchange, or reverse engineer, disassemble, or decompile the Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use the Exchange, in whole or in part, to a third party. Hospital in no event shall access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation. Except as expressly set forth in this Agreement, Hospital will not obtain any rights in the Exchange, Documentation, any of the technology used to create the Exchange, including electronic formats and tools that Network or Access Provider uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by Network, Access Provider, or Host to develop, maintain, and operate the Exchange and deliver services to Hospital.

sp.08-RR.05
The Receiving Party shall make its internal practices, books and records relating to its Uses and Disclosures of Protected Information Received from the Disclosing Party available to HHS, upon HHS's request, for purposes of determining the Disclosing Party's compliance with the Information Privacy and Protection Laws.

sp.08-RR.05
The Receiving Party shall promptly notify the Disclosing Party of any Use or Disclosure of the Protected Information contrary to the terms of this Agreement of which the Receiving Party becomes aware.

ph.06-RR.05
6.3.2. No Services Prohibited by Local Laws. The Data Recipient shall not use the System or the Services for which the Data Recipient has registered for any purpose or in any manner that is prohibited by the laws of the State of ____________. Without limiting the generality of the foregoing, the Data Recipient shall comply with the following: [list of state or local legal requirements, if desired].

mm.10-RR.05
Enforcement and Remedies

Document the responsible organizations for enforcing rules regarding payment, access rights, performance requirements, security, etc. associated with the XDS Affinity Domain. Clearly differentiate the areas of responsibility for the different organizations. If it is not clear who will ultimately be responsible for certain areas then also document this here.

hh.06-RR.05
Neither Network shall, or allow a registered user to, access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation.

ss.05-RR.05
As designated by the joint working group, each signatory should provide copies of their respective statutes or regulations related to public health events, infectious disease agents and other relevant material as needed to every other signatory. Each signatory should ensure that the copies so provided are accurate and current. The signatories should jointly identify and maintain in common a set of materials, which they agree reflect the applicable laws and regulations of the Governments of the United States and Canada.

ph.06-RR.05
10.1 Compliance with Laws and Regulations. The Participant’s obligations to comply with applicable laws and regulations, generally. Without limiting any other provision of the Terms and Conditions relating to the parties’ compliance with applicable laws and regulations, the Participants shall perform in all respects as contemplated by the Terms and Conditions, in compliance with applicable federal, state, and local laws, ordinances and regulations.

ph.06-RR.05
9.3 Reporting of Serious Breaches. Provisions requiring the SNO and Participant to report to each other concerning serious breaches of confidentiality of patient health information. Without limiting Section 9.4.7(Reports), if applicable to [SNO Name], [SNO Name] and Participant shall report to the other any serious use or disclosure of Protected Health Information not provided for by the Terms and Conditions of which [SNO Name] or Participant becomes aware, and any security incident concerning electronic Protected Health Information (a “Serious Breach of Confidentiality or Security”). A “Serious Breach of Confidentiality or Security” is one that adversely affects (a) the viability of the NHIN; (b) the trust among Participants or (c) the SNO's legal liability.

ph.06-RR.05
The Model assumes that the Common Framework Policies and Procedures will describe prohibited uses of the system and information access through the system that apply to the entire network, e.g., prohibitions necessary for compliance with HIPAA. The SNO may add to the list of prohibited uses in order to comply with state and local laws and/or other specific concerns of the SNO. The SNO may add prohibited uses, so long as those prohibitions are not inconsistent with the Common Framework Policies and Procedures.

ph.06-RR.05
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-RR.05
1. [State Organization] may use and disclose PHI if necessary for proper management and administration of [State Organization] or to carry out the legal responsibilities of [State Organization].

ph.06-RR.05
Each party shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally funded health care program participation or licensure which: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally funded healthcare program, including the Medicare and Medicaid programs.

mm.10-RR.05
Health care personnel from a sending signatory providing services at the request and within the jurisdiction of any receiving signatory in order to provide assistance in preventing, detecting or responding to a public health emergency shall not be held civilly liable or criminally responsible for any act or omission made in providing those services unless the act or omission is the result of willful misconduct, gross negligence or recklessness. In determining whether health care personnel have acted with willful malice, gross negligence or recklessness while engaged in providing services within and at the request of a receiving signatory, the substantive law of the sending signatory shall apply.

ph.06-RR.05
Providing customized summary reports with non-identifying data or statistics as needed for public health or other governmental purposes required by law.

RR.06 Obligation to Obtain and Maintain Compliant Software/Hardware Necessary to Utilize the HIE

ph.06-RR.06
C. [State Organization] will use appropriate administrative, technical and physical safeguards to protect the confidentiality and integrity of PHI and to prevent the use or disclosure of any individually identifiable health information received from or on behalf of Provider other than as permitted or required by Federal or State law or by this Agreement. [State Organization] agrees to comply with applicable requirements of law relating to PHI and with respect to any task or other activity [State Organization] performs on behalf of Provider to the extent that the Provider would be required to comply with such requirements.

sp.08-RR.06
C. Maintenance of Hardware
Clinic assumes full responsibility for the hardware, including resolution of any malfunctions or problems. This would include maintenance and/or replacement of computer.

ph.06-RR.06
Hospital shall acquire, install, provide, and properly maintain, at its own cost, the hardware and software including, without limitation, all of Hospital's core systems necessary or appropriate to receive, access and utilize the Exchange, as permitted by this Agreement.

ph.06-RR.06
Hospital shall be responsible for ensuring the security and confidentiality of the password protected accounts within the Exchange to which Hospital's employees are granted access in order to access and use the Exchange ("Data User Account"), including, without limitation, all user IDs and passwords assigned to such Data User Accounts. Hospital employees shall not disclose their Data User Accounts to any third party, and Hospital employees hereby are expressly prohibited from sharing their Data User Accounts with any third party.

mm.10-RR.06
Define the rules for DNS management and system naming conventions. Make sure to mandate the use of appropriate host names and policies that will attempt to guarantee their continued use as hardware is upgraded and replaced over time. This is important because host names are used in the <location> part of Metadata URLs, and thus URLs can be broken if host names are not maintained over time.

mm.10-RR.06
Data Retention, Archive, and Backup

Define policies regarding the responsibilities for data retention, archive, and backup for the various types of components of the XDS Affinity Domain. For example, specify how long access to documents published to an XDS Repository of the XDS Affinity Domain must be maintained, and how long their data integrity must be guaranteed. State the backup requirements for the Repository.

mm.10-RR.06
Service Level Agreements

Define how Service Level Agreements shall be created for the operational components of the XDS Affinity Domain.

ph.06-RR.06
10.4 Malicious Software, Viruses, and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO's System. The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including without limitation the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine, or data (including without limitation malicious software or "malware," viruses, worms, and Trojan Horses) which will disrupt the proper operation of the System or any part thereof or any hardware or software used by [SNO Name] in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by [SNO Name] or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

ph.06-RR.06
The Model assumes that the SNO will provide some of the software and hardware that Participants will require to use the System, as described in Section 8 (Software and Hardware Provided by [SNO Name]), and that the Participant will be required to provide the

remainder (e.g., a personal computer with an operating system and web browser meeting certain specifications), as described in Section 10.3 (Software and/or Hardware Provided by Participant). The terms of Section 8 (Software and/or Hardware Provided by [SNO Name]) and Section 10.3 (Software and Hardware Provided by Participant) should be revised as necessary to conform to each other.

ph.06-RR.06
10.3 Software and Hardware Provided by Participant. Provision requiring the Participant to obtain and maintain all hardware and software required to use the System and the Services that is not to be provided by the SNO. Each Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the Services (including the Associated Software), and provide to [SNO Name] all information required to be provided by the Participant ("Participant's Required Hardware and Software"). Each Participant's Required Hardware and Software shall conform to [SNO Name]'s then-current specifications. [SNO Name] may change such specifications from time to time in its sole discretion upon not less than sixty (60) days prior notice to each Participant affected by the change. As part of the Participant's obligation to provide Participant's Required Hardware and Software, the Participant shall be responsible for ensuring that all the Participant's computers to be used to interface with the System are properly configured, including but not limited to the operating system, web browser, and Internet connectivity.

ph.09-RR.06
10.3 Software and/or Hardware Provided by Participant. Provision requiring the Participant to obtain and maintain all hardware and software required to use the SNO's System and Services that are not to be provided by the SNO.

10.4 Viruses and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO's System.

10.5 Training. A description of the training, if any, that the SNO will require the Participant to provide to its personnel.

SNO Operations and Responsibilities. Provisions describing the role and responsibilities of the SNO.

11.1 Compliance. The SNO's obligations to require that all Participants agree to be bound by the SNO Terms and Conditions.

11.2 Training. The SNO's obligations to provide training for Participants and/or their Authorized Users.

11.3 Telephone and/or E-Mail Support. The SNO's obligations to provide support for the Participant's use of the SNO's System and/or Services.

11.4 Audits and Reports. Audits the SNO is to perform, and reports it is to provide, to Participants.

11.5 Management Committee. Any role Participants would have in governance or decision-making by the SNO.

11.5.1 Composition. The composition of a body in which Participants would be involved.

11.5.2 Meetings and Responsibilities of Management Committee. The responsibilities of such a body and how often it would meet.

11.5.3 Management Committee Bylaws. How this body would be organized and governed.

12. Fees and Charges. Terms regarding amounts, if any, that the Participant will be required to pay to the SNO in order to use the Services.

pp.06-RR.06
Section 8.04 Agents and Subcontractors. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of, a Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to the Business Associate with respect to PHI.

mm.10-RR.06
Each signatory undertakes to provide to every other signatory divisible or duplicate health data relevant to a deadly agent or public health emergency. Health data shall be transmitted in the form employed or maintained by the sending signatory or in such other form as agreed.

Protection of health data

RR.07 Miscellaneous Recipient Requirements Provisions

pp.06-RR.07
(b) Recognizing the value of allowing broad access to health information to treat patients, a Full Participant may also propose to the other Participants (through the Management Committee) to allow physician practices whose physicians are on staff at a Full Participant to have access to the Information for Treatment encounters that occur outside of the boundaries of the Full Participant (e.g., for affiliated physician office visits). Each Participant, through its Management Committee representative, may decide whether to allow such access and shall inform the Management Committee of such a decision. The Full Participant requesting such access shall be responsible for ensuring that the members of the physician practice group agree to and comply with the conditions set forth in Section 4.04.

mm.06–RR.07
Network member hospitals shall notify the Exchange and Access Provider and/or Host in advance of any planned changes in their legacy system, firewalls or VPN that may impact the data accessed by Exchange or the connectivity to Exchange.

pp.06-RR.07
Section 4.05 Access Reporting to Participants. Upon request, [Organization] shall provide to each Participant statistical summaries indicating the number of accesses to the requesting Participant’s own Information by accessing site and including a list of all queries to the Network by patient names and date of birth. The foregoing summaries shall be provided at no cost. Additional detail about a Participant's own Information may be obtained by a Participant at a reasonable fee in compliance with the provisions of this Agreement.

pp.06-RR.07
Section 6.01 [Organization] Role. [Organization] shall administer the Network and may delegate responsibilities related to Network administration to one or more subcontractors. [Organization] shall obtain adequate assurances from its subcontractors that only specifically authorized representatives of the subcontractor shall be granted access to the Network in connection with the subcontractor’s responsibilities. The Participants acknowledge and agree that access to data (including aggregate data) shall be granted to

[Organization] for all of its functions and obligations under this Agreement and shall be granted to [Organization]'s subcontractors for the sole purpose of assisting [Organization] in maintaining the technical operations of the Network. The Participants acknowledge that [Hospital] is currently a subcontractor of [Organization] for purposes of assisting [Organization] in the maintenance of the Network by installing new operating systems, defining networks, performing data backup functions, and assisting with hardware problems. While it is contemplated that [Hospital] will continue to perform these functions, should [Organization] require a different or additional subcontractor, such a subcontractor shall be subject to the approval of the Management Committee pursuant to Section 10.02, unless [Organization] performs such functions itself. [Organization] shall employ security mechanisms that are consistent with the final Security Standards (45 CFR Parts 160, 162, and 164) issued pursuant to the Health Insurance Portability and Accountability Act of 1996 to provide for the security of the Information.

pp.06-RR.07
Section 7.01 Review of Research Requests.

(a) [Organization], from time to time, may act as Participants' Business Associate for purposes of reviewing requests for the use and disclosure of the Information for research purposes that are submitted to [Organization] and may use and disclose Information in accordance with this Article. When [Organization] reviews a research proposal or project for the use of Information, [Organization] will verify the identity of the person or entity requesting the Information and also verify the authority under which the request for Information is made.

Any research proposal that [Organization] reviews pursuant to Section 7.01(a) that proposes to use all or any subset of the Information must contain at least: (a) the name(s) of the sponsor(s) of the research and the name(s) of any institution(s) under whose auspices the sponsor(s) is working; (b) the specific question to be addressed by the research (no researcher shall be permitted to access the Information without identifying a targeted goal for the research); (c) the Information to which access is requested; (d) the proposed use of said Information; (e) whether the research will require the identification of specific patients; (f) whether the research will require the identification of specific Participants; (g) any proposed publication of the results of the research; and (h) the means for protecting the confidentiality of the Information.

[Organization] shall require third parties to warrant that research publications arising from the use of Information under this ARTICLE VII will contain only aggregate data and will not specifically identify any patient whose Information is received pursuant to this Agreement unless a specific authorization to do so is obtained from a patient.

Section 7.02 Specific Pre-Approved Research Projects. The Parties acknowledge that certain research projects are ongoing at the time of the execution of this Agreement and the use and disclosure of Information for such projects have been approved by the Participants and appropriate Institutional Review Boards. Therefore, the Parties agree that Information may be used and disclosed, consistent with the appropriate Institutional Review Board approval, for the following projects:

(a) [Organization] may use and disclose the Information for the purposes originally outlined and approved by the contract between [State] University and the National Institutes of Health through the National Library of Medicine providing for the creation and maintenance of an [State Network Name].

(b) [Organization] may use and disclose the Information for purposes related to the [Network Name] supported by the National Cancer Institute and with which each of the Participants have a subcontract.

Section 7.03 Other Research By [Organization] or Third Parties.

General Rule – Approvals Required. Except as otherwise provided below in this Section 7.03, any use or disclosure of the Information (whether in identified or deidentified form) for research not allowed by Section 7.02 (Pre-Approved Projects for Research Uses and Disclosures), shall be proposed to the Management Committee and approved by: (1) an Institutional Review Board designated or approved by [Organization]; (2) the Management Committee Representatives of any Participant whose Information is used in the research; and (3) [Organization]. Prior to allowing the use of its Information for research purposes, a Participant may require that the project be subjected to the review of an Institutional Reviewing Board of its own choice. A Participant may decline to allow its Information to be used for a particular research study, but that shall not preclude the use or disclosure of the remaining Participants' Information for such project.

No Further Approvals Required – Independent Agreements Between Participants and [Organization]. If [Organization] has entered into, or enters into, any other agreement with one or more Participants that complies with the Privacy Rule with regard to the research uses and disclosures of the Participant's own Information stored on the Network, the provisions of such an agreement shall govern the use and disclosure of that Participant's Information and the approvals required by Section 7.03(a) shall not be required.

No Further Approvals Required – Preparatory to Research and Decedents' Research. [Organization] (as Participants' Business Associate) may, and the Participants (as Covered Entities) hereby delegate the authority to [Organization] to, authorize the use or disclosure of Information (whether in identified or deidentified form) for research projects without further approval from Participants under Section 7.03(a), if the research projects meet the following criteria (provided that all Privacy Rule requirements regarding research have been met, including, but not limited to, the guidelines set forth in Section 7.04):

[Organization] may use or disclose identifiable PHI for reviews preparatory to research (consistent with 45 CFR § 164.512(i)(1)(ii)); and

[Organization] may use and disclose identifiable PHI for research on decedent's information (consistent with 45 CFR § 164.512 (i)(1)(iii)).

At the request of a Participant, [Organization] shall provide reports of the research disclosures made pursuant to this Section.

(d) No Further Approvals Required – Certain Disclosures of Deidentified Information and Limited Data Sets. [Organization] (as Participants' Business Associate) may, and the Participants (as Covered Entities) hereby delegate the authority to [Organization] to, authorize the use or disclosure of deidentified Information or Limited Data Sets to any entity that has obtained an approval from an Institutional Review Board acceptable to [Organization] for the use of deidentified Information or Limited Data Sets in connection with a research project. Further, [Organization] may use or disclose deidentified Information or Limited Data Sets without further approval from a Participant if such deidentified Information or Limited Data Sets are included in classes or categories of queries that are approved by the Management Committee or an Institutional Review Board acceptable to [Organization]. At the request of a Participant, [Organization] shall provide reports of the research disclosures made pursuant to this Section.

pp.06-RR.07
Section 7.05 Involvement of Participant Investigator in Research. As a condition of approval of a research project not conducted by [Organization], any sponsor of research using all or any subset of the Information shall be required to invite an investigator from any Participant whose Information is used in the research and an investigator from [Organization] to participate in the research project.

Section 7.07 Cooperation by Participants' in Network Evaluations. The Participants agree to cooperate in studies conducted from time to time by the [Organization] related to various issues surrounding the Network, including, but not limited to, the efficacy and usefulness of the Network. Such cooperation by the Participants may include, but not be limited to, participation in interviews, the completion of surveys, and the submission of other written or oral evaluations.

pp.06-RR.07
Section 8.03 Report of Improper Use or Disclosure. Business Associate agrees promptly to report to a Covered Entity any use or disclosure of the Covered Entity's PHI not provided for by this Agreement of which Business Associate becomes aware.

sp.07-RR.07
I must obtain a written authorization from the individual for the use and disclosure of protected health information unless the disclosure is to the individual, for treatment, payment, or the disclosure falls under a specified exception.

sp.07-RR.07
ss.07-RR.07
Facilities must obtain a written authorization from the individual for the use and disclosure of protected health information unless the disclosure is to the individual, for treatment, payment, or health care operations, or the disclosure falls under a specified exception.

sp.07-RR.07
ss.07-RR.07
The facility will assign an account administrator to be responsible for this facility's [Immunization system] account. The account administrator will be responsible for the following:

- Creation of additional individual user accounts to be assigned to this facility.
- Setting or changing each user's access level.
- Immediately removing access to [Immunization system] for users who leave your employment.
- Notification to [Immunization system] of any facility changes such as site name, address, phone/fax number, account administrator, or the closing of the facility.

sp.09-RR.07
Suggestions for developing contract clauses for sponsored research projects that permit broad data sharing, including the use, when appropriate,of model contract clauses (see below).

sp.09-RR.07
Informational documents for IRB use in reviewing proposals for data sharing via the [State Organization] infrastructure that utilizes, when appropriate, the [State Organization] data sharing plan guidelines.

sp.09-RR.07
Standardized click-through agreements between data providers and users (e.g., data-related provisions in Data Use Agreements and Material Transfer Agreements).

sp.09-RR.07
Model researcher questionnaires and data sharing checklists.

sp.09-RR.07
Model contract clauses for sponsored research projects (including clinical trial agreements) to permit data sharing.

sp.09-RR.07
Facilitate and expedite the arrangements between institutions to share data.

sp.09-RR.07
Best practices, suggested conduct, and proposed recommendations that will inform the researcher and the institution of the advantages of sharing data and community-developed methods for encouraging and recognizing data sharing among researchers across departments within a single institution and located at different institutions.

sp.09-RR.07
Model agreements and other documents will expedite the negotiations between institutions for sharing data by providing simple standard agreements for most low and medium sensitivity data sets.

sp.09-RR.07
The Center will be expected to participate in the evaluation and refinement of model documents, to pilot their use for internal processes, and provide recommendations for further refinement based on such experience.

sp.09-RR.07
The Center will be expected to participate in the evaluation and refinement of best practices and suggested guidance documents, to pilot their use for internal approval processes, and to provide recommendations for further refinement based on such experiences.

ph.02-RR.07
a. PROVIDER/REPOSITORY may use data owned by the Data Provider to create limited data sets including the elements set forth in Appendix A, and may disclose such limited data sets to RESEARCHER or its authorized contractors subject to this Agreement.

mm.07-RR.07
This policy applies to the following personnel: all persons who receive access to [State Organization] through the Provider, including, but not limited to, medical records personnel, information technology and support center personnel, medical staff, and employees involved in health care operations. This policy covers the minimum necessary standards for identification and verification of persons permitted to access [State Organization]. Providers who participate in [State Organization] may enact procedures that are more stringent than this policy, but must not allow those procedures to conflict with, or be less restrictive than this policy.

mm.07-RR.07
This policy applies to any person permitted to access [State Organization] through this entity’s access portal. It does not apply to patients or clients of this entity, who will be

supplied access individually through [State Organization]. Each person accessing [State Organization] must be verified prior to receiving a passcode or other necessary tools for access to the system. Because this system is allowing access to health information not owned or controlled by this entity, the general exceptions to required verification, such as exceptions for clergy, do not apply.

mm.07-RR.07

a. Prior to receiving a passcode or other necessary tools for accessing [State Organization], a person must have both their identity and authority verified in accordance with the procedures described below.

b. The following forms of identification are sufficient for verifying a person's identity:

- Official and valid state ID (driver's license, state ID card);
- Official and valid federal ID (passport, military or government ID); or
- Official and valid entity-issued picture ID.

c. The following items are sufficient for verifying a person's authorization to access [State Organization]:

- Entity-issued ID indicating authorization to access [State Organization];
- Authorization on official entity letterhead from the Privacy Officer or other person designated to determine access levels for [State Organization]; or
- Email authorization from the official entity email address of the Privacy Officer or other person designated to determine access levels for [State Organization].

d. If a person provides sufficient documentation to meet the requirements of subsections (b) and (c) above, a passcode or other necessary tools for accessing [State Organization] may be issued. At the time of issuance, the person supplying the passcode or other necessary tools should place a copy of the identification and authorization documents in the designated [State Organization] Verification File.

e. If a person provides any other type of identification or authorization (student ID, court order, etc.), please contact the Privacy Officer or other person designated by this entity to determine access levels for [State Organization].

f. The majority of persons requiring access to [State Organization] should have their identification and authorization verified prior to any necessary use of the system. For this reason, emergency access to [State Organization] should not be necessary. If, however, a person requests emergency access, the entity should contact an on call provider with access to the system to assess the totality of the situation on a reasonableness basis.

mm.07-RR.07

Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers may also be required to provide [State Organization] with a list of active staff members with access to [State Organization], in accordance with the Provider Participation Agreement. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

b. Patient desires to obtain access personally and permit authorized users of their choice to use the Network and the information and databases supplied by all providers participating in the Network (the Databases") and, accordingly, has completed and executed the necessary portions of this Agreement, as well as reviewing and agreeing to the various policies of the Network.

ph.06-RR.07
Provider agrees to supply [State Organization] with copies of the applicable privacy and security policies and procedures of its organization upon signing of this Agreement. The Provider may also be asked at any time to provide evidence of compliance with [State Organization] policies, and to validate that appropriate organizational policies and procedures are in place to comply with those policies. If a Provider needs assistance with such policies and procedures, it should notify [State Organization] prior to entering into this Agreement, and [State Organization] will provide assistance to the extent that such resources are available.

ph.06-RR.07
Provider agrees to regularly monitor and audit access to [State Organization] and report any issues to [State Organization] upon discovery. Provider shall immediately notify [State Organization] of the revocation of an individual's access and will provide a follow-up report regarding the breach/violation within sixty (60) days of such breach/violation.

ph.06-RR.07
Provider agrees to supply [State Organization] with the names of any persons who are given access to the Network, and a quarterly list of the active staff with access to the Network (due by the 15th of January, April, July and October). Provider should be aware, and should make potential employees aware, that individuals may be denied access to the Network based on past performance or behavior reported by a former employer or other participating provider.

mm.06-RR.07
This policy applies to the following personnel: all persons who receive access to [State Organization] through the Provider, including, but not limited to, medical records personnel, information technology and support center personnel, medical staff, and employees involved in health care operations. Providers who participate in [State Organization] may enact procedures that are more stringent than this policy, but must not allow those procedures to conflict with, or be less restrictive than this policy.

mm.06-RR.07
The Provider will discipline, as appropriate, any person who violates the Provider's security policies and procedures and/or causes the Provider to violate the Provider Participation Agreement with [State Organization].

mm.06-RR.07
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

ph.09-RR.07
5. Authorized Users. Terms that govern use of the SNO Services by the Participant's Authorized Users. The Model assumes that "user agreements" will not be required of every individual who uses the SNO's System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO's System and Services ("Authorized User").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will use the SNO's Services.

5.2 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users.

5.3 No Use by Other than Authorized Users. A requirement that the SNO's System and Services be accessed and used only by Authorized Users.

5.4 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users.

6. Data Recipient's Right to Use Services. Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services). Provisions that apply specifically to "Data Providers"(i.e., Participants registered to provide data to the SNO) appear at Section 7 (Data Provider's Obligations).

6.1 Grant of Rights. The nature of the Participant's right to use the System and Services.

6.1.1. Grant by SNO. The rights granted by the SNO.

6.1.2. NHIN. The rights granted by the NHIN.

6.2 Permitted Uses. The permitted uses of the SNO's System and Services.

6.3 Prohibited Uses. The prohibited uses of the SNO System and the SNO Services applicable under the Common Framework Policies and Procedures, and additional prohibitions imposed by the SNO, if any.

7. Data Provider's Obligations. Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data). Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services) appear at Section 6 (Data Recipient's Right to Use Services).

7.1 Grant of Rights. The nature of the Data Provider's right to use the System.

7.2 Provision of Data. Terms that apply to the Data Provider's delivery of data to the Network, e.g., format, standards, etc.

7.3 Measures to Assure Accuracy of Data. The Data Provider's obligations to provide accurate, complete, and timely information.

7.4 License. The Data Provider's agreement that the data it provides will be available for use through the Network.

ph.02-RR.07

a. PROVIDER/REPOSITORY may use data owned by the Data Provider to create limited data sets including the elements set forth in Appendix A, and may disclose such limited data sets to RESEARCHER or its authorized contractors subject to this Agreement.

ph.06-RR.07

3.1 Generally. The Terms and Conditions apply to the operation of the System, the provision of the Services, and the relationships among [SNO Name] and Participants with respect thereto.

ph.06-RR.07
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

ph.06-RR.07
4.3 Online Registration. How Participants may register online.

ph.06-RR.07
4.3.2 Participant Type. How the SNO will categorize Participants by their respective roles in the health care system. Each registrant shall register to participate in one of the following Participant Types: (a) Physician or medical group; (b) Laboratory; (c) Hospital; (d) Public health agency; (e) Pharmacy; (f) Pharmacy benefit manager; (g) Health plan, insurer or other payor; (h) Researcher; and (i) [additional or different provider types selected by the SNO, subject to any limits imposed by the Common Framework Policies and Procedures].

ph.06-RR.07
4.3.3 Approval and Disapproval of Registration Forms. The SNO will be entitled to review all registration forms and decide not to accept any given party's registration. [SNO Name] shall review each Registration Form and shall approve or disapprove each in accordance with the Terms and Conditions and as [SNO Name] determines in its sole discretion is appropriate. [SNO Name] shall not be required to approve any Registration Form or other application to be a Participant.

ph.06-RR.07
The Model is drafted to provide the SNO maximum flexibility in controlling who may become a Participant. The SNO may wish to reserve the right not to register a particular Participant if, for example, the SNO determines that the person is not eligible to participate or is not expected to comply with the SNO Terms and Conditions. In addition, the SNO may wish to adopt specific credentialing criteria for Participants, which may, if desired by the SNO, be set forth in the SNO Terms and Conditions. The SNO may wish to consider whether it wishes to disclose to an unsuccessful applicant the bases upon which its application for registration was not approved.

ph.06-RR.07
The Model assumes that the Participant will be permitted to select its Authorized Users without review or approval by the SNO. The SNO may, however, wish to adopt specific credentialing criteria for Authorized Users that would be administered by the SNO, and which may, if desired, be set forth in the SNO Terms and Conditions. The Model assumes that Participants will be required to inform the SNO of changes to their lists of Authorized Users on an ongoing basis. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users.

ph.06-RR.07
5.3 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users. Based on the information provided by the Participant pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized

User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

ph.06-RR.07
5.5 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users. The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant's Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant's Authorized Users, with respect to the System, the Services and/or any confidential and/or other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant.

ph.06-RR.07
6.1.2 Applicable Common Framework Policies and Procedures. The terms of the Common Framework Policies and Procedures that apply to a Data Recipient's right to use the SNO Services and ownership of the network and information obtained through the network. All issues concerning the ownership and rights in the NHIN and data and information obtained there from shall be as set forth in the Common Framework Policies and Procedures, which is incorporated herein by reference.

ph.06-RR.07
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:]

ph.06-RR.07
10.5 Training. A description of the training, if any, that the SNO will require the Participant to provide to its personnel. The Participant shall provide appropriate and adequate training to all of the Participant's personnel, including without limitation Authorized Users, in the requirements of applicable laws and regulations governing the confidentiality, privacy, and security of protected health information, including without limitation requirements imposed under HIPAA.

ph.06-RR.07
11.6 Management Committee. Certain SNOs may wish to include certain terms regarding internal governance and management as a part of the SNO Terms and Conditions, to assure that Participants may be involved in their governance and/or management. The language provided here is for illustration only, and is not intended to limit how the SNO would structure its governance or Participants' involvement in governance and management. SNOs that do not desire such provisions would omit this section entirely.

ph.06-RR.07
11.6.1 Composition. [SNO Name] shall create and maintain a Management Committee (the "Management Committee") composed of [specified personnel/representatives of SNO and specified number of Participant representatives, who shall be selected in a specified manner].

ph.06-RR.07
11.6.2 Meetings and Responsibilities of Management Committee. The Management Committee shall meet [describe intervals, e.g., monthly] to consider and resolve various issues pertaining to the use of the System and the Services by Participants, including [list].

ph.06-RR.07
Issues that a Management Committee could address include, without limitation, technical issues, confidentiality, the scope of information stored and accessed by Participants, the use of the information, changes to the Terms and Conditions, and any other issues related to the network or the parties' participation therein.

ph.06-RR.07
11.6.3 Management Committee Bylaws. The Management Committee shall adopt bylaws for the conduct of its meetings and other proceedings.

ph.06-RR.07
2. Review of Application

[SNO Name] will review this application for registration and may accept or reject this application in accordance with the terms and conditions set forth in Section __ of the [SNO Name] Terms and Conditions. Upon [SNO Name]'s acceptance of this application, [SNO Name] shall notify the Applicant and shall register the Applicant as a [Participant]. [Optional, if SNO is to issue passwords:] [SNO Name] shall issue each Participant a [User I.D. and] password to access and use the [SNO Name] System and the [SNO Name] Services.

ss.05-RR.07
The signatories will maintain a joint working group to confer at least annually for the purpose of reviewing and maintaining the procedures by which to share the information necessary for an effective response to a public health event and to conduct joint communication and coordination of information before and during a public health event. Such procedures are set out in the most recently approved "[Region] Health Initiative Infectious Disease Emergency Communications Guideline."

mm.10-RR.07
Management When Systems are Unavailable

Define policies for managing cases where various types of components of the XDS Affinity Domain are unavailable. For example, what type of workarounds should be used if the PIX Manager for this XDS Affinity Domain implementation is unavailable? Other considerations include, but are not limited to Notification mechanisms for scheduled system downtime and maintenance; Notification of causes and resolutions for unscheduled system downtimes.

mm.10-RR.07
Affinity Domain Actors

A number of systems implementing IHE Actors defined in the XDS Integration Profile need to be identified and configured to communicate. This includes defining addressing information and ATNA Secured Node certificate.

mm.10-RR.07
Registry

Identify any specific requirements for a Registry Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
Repository

Identify any specific requirements for a Repository Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
Document Consumers

Identify any specific requirements for a Document Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework**.**

mm.10-RR.07
PIX Patient Identity Source

Identify any specific requirements for a PIX Patient Identity Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
PIX Manager

Identify any specific requirements for a PIX Manager Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
PIX Consumer

Identify any specific requirements for a PIX Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
PDQ Source

Identify any specific requirements for a PDQ Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-RR.07
PDQ Consumer

Identify any specific requirements for a PDQ Consumer Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

Audit Repository

mm.10-RR.07
Identify any specific requirements for an Audit Repository Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework. Specify any requirements for security audit logs that go beyond those specified in the ATNA Profile.

mm.10-RR.07
XDS Affinity Domain Transaction Support

Specify any details required for transactions within this XDS Affinity Domain.

mm.10-RR.07
XDS Affinity Domain Transaction Diagram

Define the transaction diagram for the XDS Affinity Domain. In particular, it is important to detail any optional transactions that the XDS Affinity Domain extensions now define as being mandatory.

mm.10-RR.07
Cross XDS Affinity Domain Transaction Support

Specify any details required for transactions from this XDS Affinity Domain to any components of another XDS Affinity Domain. Explain procedures for dealing with the use of different code sets. Also explain how to deal with the validity of assigning authorities for identifiers from external systems.

sp.08-RR.07
The [Immunization] Registry Security and Confidentiality Agreement must be signed by a representative of the participating health care entity or school, prior to any training on use of the [Immunization] Registry and gaining access to the Registry data. One or more persons from each site must complete the training for the [Immunization] Registry Site Administrator(s). Having completed the training, the Site Administrator(s) may enroll users who have been trained in the use of the [Immunization] Registry at the appropriate access level and have signed the [Immunization] Registry User Security and Confidentiality Agreement. The [Immunization] Registry Coordinator will maintain a file of signed [Immunization] Registry User Security and Confidentiality Agreements and will require new agreements to be signed by users every two years. The participating health care entity or school assumes responsibility for the individual's usage of the [Immunization] Registry. Providing access to [Immunization] Registry to outside organizations is strictly forbidden.

sp.08-RR.07
Only personnel whose assigned duties include functions associated with the immunization of children can be given access to Registry information. All personnel including permanent and temporary employees, volunteers, contractors, and consultants will be required to sign a [Immunization] Registry User Security and Confidentiality Agreement before gaining access to the Registry. Whenever a user terminates the employment or other status, that person's [Immunization] Registry user account must be removed immediately. A user taking an extended leave of absence must have the account status set to Inactive. Users who fail to access the [Immunization] Registry for more than 60 consecutive days will have their accounts inactivated by [Immunization] Registry.

mm.08-RR.07
Access to the Registry will be allowed only through Registry approved access procedures. Each person granted access to the [Immunization] Registry must have a unique login ID

and password. Shared login IDs and passwords will not be permitted. Users are prohibited from disclosing Registry access codes or protocol to unauthorized persons. Site administrators will ensure that users have been adequately trained to use the Registry and are not given any higher level of access than that necessary to perform their assigned duties.

ph.06-RR.07
Hospital License and Restrictions. Subject to the terms and conditions of this Agreement and during the term of this Agreement, the Hospital is hereby granted a limited license to allow its Authorized Users (as defined in Exhibit A) to remotely access and use the Exchange and Documentation for the sole purpose of accessing and viewing Data in the Exchange as authorized by Network. Any access to or use of the Exchange not expressly permitted in this Agreement is prohibited. Except as expressly permitted in this Agreement, Hospital shall not, and shall not allow or authorize any third party to: (i) use or access to the Exchange; (ii) alter, enhance or otherwise modify, or create derivative works of the Exchange, or reverse engineer, disassemble, or decompile the Exchange or any of its components; or (iii) sublicense, transfer, or assign its rights to access and use the Exchange, in whole or in part, to a third party. Hospital in no event shall access, transfer, use, or disclose Data in any manner or for any purpose that is prohibited by any applicable state or federal law, rule, or regulation. Except as expressly set forth in this Agreement, Hospital will not obtain any rights in the Exchange, Documentation, any of the technology used to create the Exchange, including electronic formats and tools that Network or Access Provider uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by Network, Access Provider, or Host to develop, maintain, and operate the Exchange and deliver services to Hospital.

sp.08-RR.07
Notify the Receiving Party immediately in the event of any proven or suspected incident in which the Disclosing Party has reason to believe any Unauthorized person may have had Access to the computer or computer systems of the Receiving Party; and

sp.08-RR.07
Conduct assessments of the policies, procedures and systems used by the Receiving Party to fulfill the obligations of this Section, (i) no less frequently than once each year, and (ii) in response to any material breach of security within the scope of this Section.

ph.06-RR.07
Hospital shall provide its employees who are granted Data User Accounts with education and training on HIPAA requirements to maintain the confidentiality of patient information accessed through Exchange.

mm.06–RR.07
Each Network member hospital will be responsible for initiating, updating, monitoring, controlling, and removing or suspending access of its Authorized Users in Exchange.

mm.06-RR.07
Once the enrolling hospital provides an Authorized User with training to familiarize them with Exchange, the enrolling hospital will assign him or her a (i) User ID that contains the abbreviation of the hospital (see below), the user’s first initial, and the user’s last name (e.g., RHJ Jones); and (ii) password that contains at least 7 digits including at least 2 alpha digits and 2 numeric digits. Authorized Users must change their passwords at least every 180 days and may not re-use a password. Passwords shall be case sensitive.

mm.06-RR.07
The first time an Authorized User logs into Exchange, he/she will view an Exchange Agreement detailing the permitted uses of the system, HIPAA compliance requirements and the user's roles and responsibilities. The Authorized User must click "I Agree" to continue using Exchange. Each Authorized User's consent to the agreement will be logged in the audit trail. The Authorized User may print a copy of the Agreement from their "preferences" section in Exchange.

The enrolling hospital immediately shall remove an Authorized User's access to the Exchange if the user is no longer employed or otherwise associated with the hospital.

mm.06-RR.07
Network member hospitals shall notify the Exchange and Access Provider and/or Host in advance of any planned changes in their legacy system, firewalls or VPN that may impact the data accessed by Exchange or the connectivity to Exchange.

mm.06-RR.07
C. Response to Patient Requests

1. When responding to requests for release of patient information, Network member hospitals shall not release data accessed or obtained through Exchange. Each hospital shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient's medical record and the system does not maintain patient data. Exchange simply queries and collates patient data from the participating providers.

sp.08-RR.07
The Receiving Party may only Disclose Protected Information to Third Parties under the following conditions:

The Disclosure is of the Minimum Necessary Information for the purposes of the Disclosure; and The Disclosure

A Is necessary to accomplish a Purpose for which the Protected Information was Disclosed to the Receiving Party, and
B Is to a Subcontractor who has entered into a Written agreement which

I Requires the Subcontractor to Protect such Information under conditions consistent with and providing at least as much Protection for the Protected Information as this Agreement, including but not limited to provisions requiring the Subcontractor to promptly notify the Receiving Party of any Use or Disclosure of the Protected Information contrary to the terms of the Written agreement under which the Receiving Party Disclosed the information; and
II Includes provisions stating that the Subcontractor shall not be deemed to have an ownership interest in the Protected Information, and requiring the Subcontractor to return, destroy or archive all such information under terms consistent with Section G of this Agreement, upon the termination of the Receiving Party's agreement with the Subcontractor; or

The Disclosure is required by law, provided that the Receiving Party shall give the Disclosing Party prior Written notice and an opportunity to intervene (unless the Receiving Party is prohibited from giving such notice by order of a court of competent jurisdiction); or
The Disclosure is to the Individual who is the subject of the Protected Information; or
The Disclosure is otherwise permitted under applicable Information Privacy and Protection Laws.

The Receiving Party shall at all times Protect information Received from the Disclosing Party in compliance with all applicable Information Privacy and Protection Laws.

sp.08-RR.07
Computer System Administration. In the event the Receiving Party Receives, Discloses, stores or Processes Protected Information using a computer or computer systems, the Receiving Party shall:
Maintain a designated individual or individuals to serve as security officer(s) responsible for supervising the security of the Receiving Party's computer systems, who shall further be responsible for communicating with the Disclosing Party with respect to matters affecting the security of the Disclosing Party's computer or computer systems;

Privacy Practices. During the Term of this Agreement the parties shall at all times coordinate any policies, processes and procedures they maintain under which Individuals are permitted to inspect, copy and amend or seek amendment of Protected Information which pertains to them. The parties shall therefore at all times:

Privacy Officers. Maintain a designated individual or individual(s) who shall be responsible (a) for ensuring the compliance of the party with the privacy requirements of all applicable Information Privacy and Protection Laws, and (b) for communicating with the other party with respect to matters concerning the inspection, copying and amendment of Protected Information by Individuals.

4.5 Provider Requirements (PR)

PR.01 Acceptance of Grant of Right/License to Use the HIE

ph.06-PR.01
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network to have access to his or her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.
- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-PR.01
5.2 Certification of Authorized Users. How the Participant will provide assurances that its Authorized Users have been trained appropriately. At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User: (a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training); (b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type); (c) Has agreed not to disclose to any other person any passwords [and/or other security

measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms); (d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and (e) [Others, if desired].

ph.06-PR.01
4.3.3 Approval and Disapproval of Registration Forms. The SNO will be entitled to review all registration forms and decide not to accept any given party's registration. [SNO Name] shall review each Registration Form and shall approve or disapprove each in accordance with the Terms and Conditions and as [SNO Name] determines in its sole discretion is appropriate. [SNO Name] shall not be required to approve any Registration Form or other application to be a Participant.

ph.06-PR.01
4.2 Registration by Agreement. How Participants may enter into a written Registration Agreement with the SNO. A person may register with [SNO Name] as a Participant by entering into a written Registration Agreement with [SNO Name]. Such a Registration Agreement shall describe: (a) the Participant's Participant Type, as described in Section 4.3.2 (Participant Type); (b) whether the Participant is a Data Provider or a Data Recipient, or both; (c) if the Participant is registered as a Data Recipient, which of the Services the Participant may use; and (d) such other terms and conditions as [SNO Name] and the Participant shall agree.

ph.06-PR.01
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

ph.06-PR.01
4.3.1 Registration Form. How the SNO administers online registration. Each person wishing to register online to access the System and use the Services as a Participant shall complete the Registration Form provided by [SNO Name] at [insert web address]. [SNO Name] may change its Registration Form at any time. A person's Registration Form shall be that person's application to become a Participant.

ph.06-PR.01
4.3.4 Acceptance of Registration. How registration agreements will be created for online registrants. Upon [SNO Name]'s acceptance of a Registration Form, that Registration Form will be the Participant's Registration Agreement and shall be legally binding upon [SNO Name] and the Participant as of the effective date [SNO Name] shall provide to the Participant.

ph.06-PR.01
7.1 Grant of Rights. The nature of the Data Provider's right to use the System.

ph.06-PR.01
7.1.1 Grant by [SNO Name]. The SNO's grant of a license to use the SNO System. [SNO Name] grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to

use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider's Obligations), subject to the Data Provider's full compliance with the Terms and Conditions and the Data Provider's Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

ph.06-PR.01
The Model uses the legal term "license" to describe the specific rights to be granted with respect to the use of Patient Data provided by the Data Provider. The Data Provider grants the SNO a license permitting the SNO to grant others access to the Provider's Patient Data through either the SNO or the NHIN in accordance with their respective requirements. If the SNO wishes to place restrictions on the use of data provided by Data Providers, it would add an additional section describing those additional restrictions (see Section 7.5 (Limitations on Use of Patient Data)).

ph.06-PR.01
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the [SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

sp.02-PR.01
E. In consideration of the Participant's entry into and compliance with this Agreement, [Entity] agrees to allow the Participant, and its associated Individual Providers (if applicable) access to information contained in the [Name] Registry, subject to the terms and conditions of this Agreement and the policies and procedures adopted by the [Name] Management Committee

ph.05-PR.01
The Regents shall provide User with access to certain data (the "Limited Data Set") in accordance with the terms and conditions of this Agreement.

sp.08-PR.01
State will provide the [IIS] software to Clinic for the purpose of participating in [IIS]. State will install the computer and configure the system for [IIS]. Ongoing improvements to the [IIS] software are the responsibility of State. No fee or charge will be assessed to Clinic for the initial installation, periodic upgrading, or the basic [IIS] training of Clinic personnel. Technical support for the [IIS] application will be provided by State. State will maintain a toll free number for Clinic's connection to the [IIS] database.

PR.02 Acceptance of Compliance with Other Policies/Procedures Adopted by the HIE (Current and Future)

ph.06-PR.02
3. [Participant]'s Agreement

Upon receipt of [SNO Name]'s notice that it has accepted this application, the Applicant shall be legally bound to comply with all of the terms and conditions of [SNO Name]'s Terms and Conditions that apply to [Participant] and may then commence to access and use the

[SNO Name] System and [SNO Name] Services, subject to all of the terms and conditions of this Registration Agreement and the [SNO Name] Terms and Conditions.

ph.06-PR.02
7.1.1 Grant by [SNO Name]. The SNO’s grant of a license to use the SNO System. [SNO Name] grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider’s Obligations), subject to the Data Provider’s full compliance with the Terms and Conditions and the Data Provider’s Registration Agreement. [SNO Name] retains all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

ph.06-PR.02
4.3.4 Acceptance of Registration. How registration agreements will be created for online registrants. Upon [SNO Name]’s acceptance of a Registration Form, that Registration Form will be the Participant’s Registration Agreement and shall be legally binding upon [SNO Name] and the Participant as of the effective date [SNO Name] shall provide to the Participant.

ph.06-PR.02
4.4 Effect of Terms and Conditions Upon Registration Agreements. How Participants will agree to comply with the Terms and Conditions. Each Registration Agreement shall incorporate by reference, and require that the Participant agree to comply with, the Terms and Conditions. [SNO Name] may make exceptions to this Section 4.4 (Effect of Terms and Conditions Upon Registration Agreements), in [SNO Name]’s sole discretion, pursuant to any written Registration Agreement entered into as described in Section 4.2 (Registration by Agreement).

ph.06-PR.02
The Model assumes that the SNO Terms and Conditions will contain virtually all of the material terms and conditions that apply to a Participant’s use of the SNO’s System and Services, and therefore will contain most of the terms of each Participant’s multilateral participation agreement. Under this approach, both written and online Registration Agreements will incorporate the SNO Terms and Conditions by reference and contain only those additional terms that apply to the Participant alone, e.g., the Participant’s name, whether the Participant is a Data Provider or Data Recipient or both, the Participant’s Participant Type, etc. The Model gives the SNO broad discretion to create exceptions to the Terms and Conditions, as the SNO determines necessary for particular Participants that enter into written Registration Agreements. The SNO should exercise care in making such exceptions, lest it undermine the effectiveness of the Terms and Conditions with respect to other Participants.

ph.06-PR.02
4.5 Changes to Terms and Conditions. How Participants will be aware of changes to the SNO Terms and Conditions, and will be legally obligated to comply therewith. [SNO Name] may amend, repeal and replace the Terms and Conditions at any time, and shall give Participants notice of those changes, as described in Section 3.2 (Development and Dissemination; Amendments). Subject to Section 4.6 (Termination Based on Objection to Change), any such change to the Terms and Conditions shall automatically be incorporated by reference into each Registration Agreement, and be legally binding upon [SNO Name] and the Participant, as of the effective date of the change.

ph.06-PR.02
4.3.1 Registration Form. How the SNO administers online registration. Each person wishing to register online to access the System and use the Services as a Participant shall complete the Registration Form provided by [SNO Name] at [insert web address]. [SNO Name] may change its Registration Form at any time. A person's Registration Form shall be that person's application to become a Participant.

ph.06-PR.02
4.1 Registration Required. Participants are to be registered with the SNO. Only persons who are registered with [SNO Name] as Participants shall be permitted to access the System and use the Services. A Participant may be registered as a Data Provider or as a Data Recipient or as both, as described in this Section 4 (Registration Agreements). A Participant may be registered to use some or all of the Services, as specified in that Participant's Registration Agreement.

mm.07-PR.02
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers may also be required to provide [State Organization] with a list of active staff members with access to [State Organization], in accordance with the Provider Participation Agreement. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

ph.06-PR.02
3.3 Relationship to Common Framework Policies and Procedures. The relationship of the SNO Terms and Conditions to the Common Framework Policies and Procedures. [SNO Name] has agreed to participate in the NHIN and to comply with the Common Framework Policies and Procedures (the "Common Framework Policies and Procedures"). The Terms and Conditions are intended to, and shall be construed to, comply with the Common Framework Policies and Procedures. The Terms and Conditions incorporate the Common Framework Policies and Procedures, as described herein. Any change to the Common Framework Policies and Procedures that [SNO Name] determines applies to [SNO Name] shall also be incorporated into the Terms and Conditions as of the time [SNO Name] determines is appropriate.

mm.06-PR.02
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

mm.06-PR.02
This policy applies to the following personnel: all persons who receive access to [State Organization] through the Provider, including, but not limited to, medical records personnel, information technology and support center personnel, medical staff, and employees involved in health care operations. This policy covers the minimum necessary standards for privacy and confidentiality. Providers who participate in [State Organization] may enact procedures that are more stringent than this policy, but must not allow those procedures to conflict with, or be less restrictive than this policy.

mm.06-PR.02
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

mm.04-PR.02
No Use or Disclosure By Any Party Without Written Patient Authorization Except for Privileged Care Uses

ph.06-PR.02
1. [State Organization] may use and disclose PHI if necessary for proper management and administration of [State Organization] or to carry out the legal responsibilities of [State Organization].

ph.06-PR.02
All of the terms of the [RHIO] Master Data Sharing Agreement - Terms and Conditions (“Terms and Conditions”), and the [RHIO] Policies and Procedures (“Policies and Procedures”), are hereby incorporated by reference into this Participant Registration Agreement. Words in this Participant Registration Agreement shall have the meanings given to them by the Terms and Conditions, and Policies and Procedures. Participant hereby represents and warrants that Participant, or an authorized person acting on Participant’s behalf, has read and agrees to comply with the Terms and Conditions, and Policies and Procedures.

ph.06-PR.02
Participant is a Hospital Type within the meaning of Section 4.3.2 of the Terms and Conditions. Participant shall be both a Data Provider and a Data Recipient, as such terms are used, and with such rights and obligations, as are set forth in the Terms and Conditions and the Policies and Procedures. [During the Initial Registration Period, Participant shall have the right to only such Services as [RHIO] may, in its sole discretion, make available. Participant agrees to be bound by, and to comply with, all of the provisions of the Terms and Conditions, and Policies and Procedures, and expresses such agreement by affixing its signature to this Registration Agreement. Accordingly, Participant may commence to access and use [RHIO]'s System and Services, subject to all of the provisions of this Registration Agreement, the Terms and Conditions, and Policies and Procedures.]

ph.06-PR.02
7.1.2 Applicable Common Framework Policies and Procedures. The terms of the Common Framework Policies and Procedures that apply to a Data Provider’s right to provide data through the SNO System, and ownership of the network and information obtained through the network. All issues concerning the ownership and rights in the NHIN shall be as set forth in the Common Framework Policies and Procedures, which is incorporated herein by reference.

ph.06-PR.02
7.3.1. Applicable Common Framework Policies and Procedures. The Data Provider’s obligations to comply with the applicable provisions of the Common Framework Policies and Procedures. Each Data Provider shall, in accordance with the Common Framework Policies and Procedures, use reasonable and appropriate efforts to assure that all data it provides to the System is accurate, free from serious error, reasonably complete, and provided in a timely manner.

ph.06-PR.02
7.5.1. Uses Prohibited by Policies and Procedures. The provisions of the Common Framework Policies and Procedures that apply to the use of information provided by Data Providers. Any use that is prohibited by the Common Framework Policies and Procedures.

ph.06-PR.02
9.1 Compliance with Policies and Procedures. Provisions requiring compliance with the Common Framework Policies and Procedures. [SNO Name] and each Participant shall comply with the standards for the confidentiality, security, and use of patient health information, including without limitation protected health information described in HIPAA, as provided in the Common Framework Policies and Procedures, which is incorporated herein by reference. Each Participant shall comply with such standards regardless of whether or not that Participant is a "covered entity" under HIPAA.

ph.06-PR.02
11.1 Compliance with Terms and Conditions. The SNO's obligations to require that all Participants agree to be bound by the SNO Terms and Conditions. [SNO Name] shall require that all Participants enter into a Registration Agreement or another legally binding agreement to comply with the Terms and Conditions in such form as [SNO Name] determines is appropriate.

ph.06-PR.02
All [Participants] must agree to the terms and conditions of [SNO Name]'s [Participant] Registration Agreement, which provides as follows:

1. [SNO Name] Terms and Conditions. All of the terms of the [SNO Name] Terms and Conditions are hereby incorporated by reference into this [Participant] Registration Agreement. Words in this [Participant] Registration Agreement shall have the meanings given to them by the [SNO Name] Terms and Conditions. All Applicants are required to read and agree to the [SNO Name] Terms and Conditions prior to completing this application.

sp.02-PR.02
The [Name] Management Committee may further require the Participant to comply with reasonable quality assurance procedures to assure the validity and integrity of Participant Information.

PR.03 Format of Data

pp.05-PR.03
4. If either [Entity] or the Insurer discloses information which is otherwise barred from disclosure under this Agreement pursuant to a release, the party making the disclosure shall ensure that the release is (a) in written form, with a copy retained by the disclosing party, (b) executed by a person with the legal authority to enter into such a release, (c) legally applicable to the information to be disclosed, and (d) effective on the date of the disclosure ("Release").

pp.05-PR.03
4. If either [Entity] or the Provider discloses information which is otherwise barred from disclosure under this Agreement pursuant to a release, the party making the disclosure shall ensure that the release is (a) in written form, with a copy retained in the records of the disclosing party, (b) executed by a person with the legal authority to enter into such a release, (c) legally applicable to the information to be disclosed, and (d) effective on the date of the disclosure.

ph.06-PR.03
7.2 Provision of Data. Terms that apply to the Data Provider's delivery of data to the Network, e.g., format(s), standards, etc.

ph.06-PR.03
7.2.1. Data Providers with Written Registration Agreements. How a written Registration Agreement will describe the Data Provider's obligations to provide data. If the Data Provider has entered into a written Registration Agreement with [SNO Name] pursuant to Section 4.2 (Registration by Agreement), the Data Provider shall provide the data described in that agreement.

7.2.2. Data Providers Registering Online. The terms regarding the Data Provider's obligations to provide data that apply to all other Data Providers.

ph.06-PR.03
Alternative One: Data Providers are required to provide specific data sets in specific format(s) based on their type of provider. If the Data Provider has registered with [SNO Name] online pursuant to Section 4.3 (Online Registration), the Data Provider shall participate in and maintain its connection to the System's record locator service-based, peer-to-peer network and provide through the System the information described in Schedule 7.2 (Provision of Data) as required for the Participant Type under which the Data Provider has registered under Section 4.3.2 (Participant Type) ("Patient Data").

ph.06-PR.03
OR Alternative Two: At the time of registration, Data Providers register to provide specific data sets in specific format(s). If the Data Provider has registered with [SNO Name] online pursuant to Section 4.3 (Online Registration), the Data Provider shall participate in and maintain its connection to the System's record locator, service-based peer-to-peer network and provide through the System the information the Data Provider registered to provide pursuant to the registration process ("Patient Data").

mm.09-PR.03
If the data already exist, do any or all of the data to be shared fall within the Common Rule definition of human subjects research?

mm.09-PR.03
II. Information about the data involved in the project and how they will be shared

Describe, with some specificity, the data that are intended to be shared, the source(s) of the data (e.g., mouse data, tissue bank specimens and annotations, imaged/annotated data, clinical trial or retrospective data from a study in progress, existing regular medical records, archived data).

mm.09-PR.03
The following chart describes the information that must be eliminated from a database, registry, or any other data set for the data set to be considered de-identified or a limited data set. Appropriately deidentified data sets are not regulated by the HIPAA Privacy Rule. Limited data sets may be used or disclosed for research, public health, and other limited purposes, but only by those who sign a data use agreement (signature may be written or electronic, depending on applicable state law and local institutional policy). Note that for each data element listed below, the information must be eliminated with respect to the patient and to any of the patient's relatives, employers, or household members.

mm.10-PR.03
Document Content Specialization

This section should specify any specialization of attributes and terminology to be used in the actual document content. This should be only for those attributes that are not defined as being part for Metadata.

mm.10-PR.03
Transparency

Document the manner in which accurate and timely disclosure of information will be provided by the various organizations that administer, organize, provide, and use the XDS Affinity Domain. Detail the procedures to follow in order to gain access to this information.

mm.10-PR.03
Provide guidelines regarding the types of information that organizations and individuals using the XDS Affinity Domain must be capable of providing should an audit of their participation or access be carried out.

mm.10-PR.03
Document Source

Identify any specific requirements for a Document Source Actor in the XDS Affinity Domain that are not fully specified or mandated by the IHE Technical Framework.

mm.10-PR.03
Document Update and Maintenance Policies

Detail policies regarding the modification, reading, and deletion of documents in the following sub-sections:

mm.08-PR.03
1. Identification of Binational Cases—The determination of whether or not a person with a notifiable disease is a binational case requires obtaining information which currently is not routinely gathered. States should encourage health professionals making disease notifications of the need to explore whether cases are binational, especially in settings where this is more probable (locations with considerable travel between the countries, migrant populations, etc.). In the future, public health authorities should consider the value of incorporating information specifically designed to identify binational cases with the other information to be routinely reported. Questions designed to elicit such information should be prepared as part of the implementation phase of these Guidelines.

mm.08-PR.03
3. Information on Binational Cases—When necessary, the information shared on binational cases should be sufficient to allow appropriate public health follow-up of the case to take place. In some circumstances, this may entail sharing patient identifying information. Following the public health laws and privacy regulations of both countries, information exchange needs to be handled confidentially.

mm.09-PR.03
2. Communications for Binational Outbreaks—Once a binational outbreak is identified, the appropriate public health officials should be notified, following a pre-defined communications protocol. The public health authorities from each country should share the

available data, and take a decision on the most appropriate response, including an agreement whether to initiate a binational investigation.

mm.09-PR.03
1. Binational Reporting of Notifiable Diseases—When a laboratory in one country analyzes or examines specimens from a person residing in the other country, and obtains a positive result for a reportable condition, this information needs to be routinely communicated to the appropriate public health officials where the tested individual resides. The mechanism for making this communication needs to be determined by state public health agencies working in coordination with public and private laboratories within its jurisdiction and with its counterparts in the neighboring country.

sp.04-PR.03
Participating Clinic agrees to provide [Program]-authorized breast and cervical cancer screening services, and diabetes and cardiovascular disease screening services, to participants, meaning women who qualify for [Program] financial assistance. Participating Clinic also agrees, as related requirements, to:

sp.04-PR.03
Provide its Tax Identification Number, for reimbursement purposes, to [Program].

Services authorized by [Program] being limited to those services listed on the attached "[Program] Payment Schedule of Allowed Services by CPT (Current Procedural Terminology) Code, Effective January 1, 2007" and "[Program] Chronic Disease Screening Program Screening Services by CPT Code and Medicare B Rate, Effective January 1, 2007." These lists may change from time to time to correspond with federal grant requirements, and Participating Clinic will be notified in writing of those changes by [Program].

sp.04-PR.03
Submit charges to any applicable insurance program or other third-party reimbursement entity prior to submitting those charges for payment by [Program]. A copy of insurance or other third-party reimbursement or denial must accompany any claim submitted for payment by [Program].

sp.04-PR.03
Submit an itemized claim to [Name], the payment intermediary for [Program], after providing authorized services to a participant. Each itemized claim must be submitted on a properly executed standardized method form, include all data elements required by [Program] and [Payment Intermediary], such as Current Procedural Terminology (CPT) codes, and meet all applicable HIPAA requirements.

sp.04-PR.03
All claims, electronic or paper, must include the [Program] Client Group Number [xxxxx].

sp.04-PR.03
Electronic claims must be submitted to the "clearinghouse" designated by [Payment Intermediary]. Participating Clinic must contact [Payment Intermediary] to determine the specific "clearinghouse" applicable to Participating Clinic.

Paper claims must be submitted to [Program] at: [Address]

Accept payment for authorized services, as described in Section A2 above, to participants as payment in full. [Payment Intermediary], as authorized by [Program], makes payment directly to Participating Clinic.

To not hold [Program] liable or responsible for any of the costs or expenses incurred in providing services to participants, except as authorized by [Program] in Section A2, submitted as required by Sections A3 to A5, and to the extent funding is available as set forth in Section B2.

ss.08-PR.03
In concept, a request for a specific patient's information will be sent (via a batch file transmission) from one collaborative partner to the other. The receiving partner's data base shall be searched to find the shared patients. A batch file will be created of the found shared patients' information and sent to the requesting collaborative partner. The requesting collaborative partner's immunization data base will be updated accordingly.

ss.08-PR.03
Immunization services in any of the forenamed locations will be sent to the electronic application specific to the Participants. Those systems are the [State]IIS, [City]CIR or the [State]SIIS. The electronic format of the data sharing/exchange will be in a format agreed upon by the Participants.

PR.04 Connection to Network

hh.06-PR.04
e. Each Network shall notify the other in advance of any planned changes in any legacy system firewalls or VPN of an Authorized User or the Network that may impact the data accessed by an Exchange or the connectivity to an Exchange.

mm.06-PR.04
Provider personnel must restrict access to [State Organization] workstations to personnel who have a legitimate and identified need to have such access, and who have been granted such access in accordance with the [State Organization] Identification and Authorization Verification Policy and Procedure.

mm.09-PR.04
3. Advanced Diagnostic Technologies—The use of advanced technologies (e.g., pulsed field gel electrophoresis) for subtyping of human and food isolates will be encouraged, as well as the sharing of findings from such technologies with counterparts in the two countries.

ph.05-PR.04
Not to use or further disclose the Limited Data Set or any information contained therein other than as permitted by this Agreement or required by applicable law.

mm.06-PR.04
Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient's data through Exchange. If a patient has chosen this option, when a query is made about that particular patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details." If a patient desires to

revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

mm.06-PR.04
Exchange automatically shall remove an Authorized User's access to the system if the user has not accessed the system during a one-year period.

sp.08-PR.04
Clinic is responsible for providing a phone line and internet connectivity. If Clinic fails to use [IIS] for three consecutive months, State reserves the right to recall the state-supplied computer and/or software.

sp.08-PR.04
Clinic is responsible for the maintenance and/or replacement costs associated with the computer and modem following expiration of the computer manufacturer's warranty. The phone line and internet connectivity are Clinic's sole responsibility.

PR.05 Accuracy of Data Provided

hh.06-PR.05
4. Data. Each Network acknowledges that the information provided through the Exchanges is drawn from numerous sources, and each Network agrees to verify, to the best of its ability, that the Data obtained from an Exchange which Authorized Users rely upon in making treatment decisions about each patient in fact corresponds to that patient.

ph.06-PR.05
Provider understands that the Network primarily depends on the participating providers to ensure that the patient information in the Databases is true, accurate and complete. If the Provider becomes aware of any inaccuracies in its own Database, it agrees to communicate such inaccuracy to [State Organization] as soon as reasonably possible.

pp.05-PR.05
4. [Entity] DOES NOT GUARANTEE THE TRUTH, ACCURACY OR COMPLETENESS OF ANY INFORMATION PROVIDED UNDER THIS AGREEMENT. THE PROVIDER IS SOLELY RESPONSIBLE FOR ITS USE OF INFORMATION PROVIDED UNDER THIS AGREEMENT IN PROVIDING HEALTH CARE, AND [Entity] WILL NOT BE LIABLE FOR ANY GENERAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES WHICH MAY ARISE OR BE CLAIMED TO ARISE FROM ANY USE OF SUCH INFORMATION.

pp.05-PR.05
4. Neither [Entity] nor the Provider shall disclose health information about an identified individual to a third party except pursuant to a release or a court order as described above in Subsections C(1) or C(2). Unless and until the following requirements are modified by processes or procedures adopted by [Entity] in the User's Manual, the party making the disclosure shall ensure that the release is (a) in written form, with a copy retained in the records of the disclosing party, (b) executed by a person with the legal authority to enter into such a release, (c) legally applicable to the information to be disclosed, and (d) effective on the date of the disclosure.

pp.05-PR.05
ii) By entering into this agreement with [Entity], the undersigned Provider will obtain the benefit of on-line access to immunization information to assist in providing health care

for its patients, including information provided or verified by other health care providers. In return, the Provider will be responsible for (a) updating immunization information as needed, (b) initiating new entries in the system upon providing immunization care to a patient for whom no pre-existing record exists, and (c) editing a record or notifying [Entity] of a potential error if the Provider has reason to believe any information contained in it is not true or accurate, or it is not complete.

pp.05-PR.05
iii) If [Entity] has reason to believe that the Provider may have provided false, materially inaccurate or materially incomplete information, or from time to time as part of an [Entity] Quality Assurance Program, [Entity] may audit the Provider to verify the truth, accuracy and completeness of the information he or she has provided. The Provider will cooperate with any such audit, which will be at [Entity]'s expense after giving reasonable notice to the Provider, and conducted with as little disruption of Provider's business as reasonably possible. All information reviewed by [Entity] for audit purposes will be kept confidential under the terms of [Entity]'s Obligation to Maintain Provider Confidentiality stated below, unless [Entity] reasonably believes disclosure is necessary to establish a claim or defense on behalf of [Entity] in a legal proceeding involving [Entity] and the Provider.

pp.05-PR.05
5. [Entity] DOES NOT GUARANTEE THE TRUTH, ACCURACY OR COMPLETENESS OF ANY INFORMATION PROVIDED UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO INDIVIDUAL PATIENT INFORMATION AND ANY TREATMENT INFORMATION AND/OR RECOMMENDATIONS PROVIDED AS PART OF THE INFORMATION SERVICES. THE PROVIDER IS SOLELY RESPONSIBLE FOR THE USE OF INDEPENDENT PROFESSIONAL JUDGMENT IN THE USE OF SUCH INFORMATION. [Entity] WILL NOT BE LIABLE FOR ANY GENERAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES WHICH MAY ARISE OR BE CLAIMED TO ARISE FROM ANY USE OF INFORMATION BY THE PROVIDER AND/OR THE PROVIDER'S EMPLOYEES, CONTRACTORS, AGENTS OR AFFILIATED PERSONS.

pp.05-PR.05
2) [Entity]'s system primarily depends upon the individual providers who use the system to ensure that the patient immunization information in the database is true, accurate and complete. In turn, providers using patient immunization information provided through [Entity] are entitled to rely upon it just as if it were part of their own patients' clinical records, whether generated by the provider's own office staff or forwarded by fax or mail from another provider's office.

pp.05-PR.05
A. The Provider's Obligation to Communicate a True, Accurate and Complete Record:

1. By entering into this agreement with [Entity], the undersigned Provider will obtain the benefit of on-line access to immunization information to assist in providing health care for its patients, including information provided or verified by other health care providers. In return, the Provider will be responsible for (a) updating immunization information as needed, (b) initiating new entries in the system upon providing immunization care to a patient for whom no pre-existing record exists, and (c) editing a record or notifying [Entity] of a potential error if the Provider has reason to believe any information contained in it is not true or accurate, or it is not complete.

pp.05-PR.05
3. If [Entity] has reason to believe that the Provider may have provided false, materially inaccurate or materially incomplete information, or from time to time as part of

an [Entity] Quality Assurance Program, [Entity] may audit the Provider to verify the truth, accuracy and completeness of the information he or she has provided. The Provider will cooperate with any such audit, which will be at [Entity]'s expense after giving reasonable notice to the Provider, and conducted with as little disruption of Provider's business as reasonably possible. All information reviewed by [Entity] for audit purposes will be kept confidential under the terms of [Entity]'s Obligation to Maintain Provider Confidentiality stated below, unless [Entity] reasonably believes disclosure is necessary to establish a claim or defense on behalf of [Entity] in a legal proceeding involving [Entity] and the Provider.

ph.06-PR.05
Provider understands that the Network primarily depends on the participating providers to ensure that the patient information in the Databases is true, accurate and complete. If the Provider becomes aware of any inaccuracies in its own Database, it agrees to communicate such inaccuracy to [State Organization] as soon as reasonably possible.

pp.05-PR.05
b. [Entity] cannot guarantee the truth, accuracy or completeness of such information. However, [Entity] will supplement, correct and validate the data upon provider notice of potential error(s).

pp.05-PR.05
4. [Entity] DOES NOT GUARANTEE THE TRUTH, ACCURACY OR COMPLETENESS OF ANY INFORMATION PROVIDED UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO INDIVIDUAL ENROLLEE INFORMATION. THE INSURER IS SOLELY RESPONSIBLE FOR THE USE OF INDEPENDENT JUDGMENT IN THE USE OF SUCH INFORMATION. [Entity] WILL NOT BE LIABLE FOR ANY GENERAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES WHICH MAY ARISE OR BE CLAIMED TO ARISE FROM ANY USE OF INFORMATION BY THE INSURER AND/OR THE PROVIDER'S EMPLOYEES, CONTRACTORS, OFFICERS, AGENTS OR OTHER AFFILIATED PERSONS.

pp.05-PR.05
III. [Entity]'s system primarily depends upon the individual providers who use the system to ensure that the patient immunization information in the database is true, accurate and complete. In turn, providers using patient immunization information provided through [Entity] are entitled to rely upon it just as if it were part of their own patients' clinical records, whether generated by the provider's own office staff or forwarded by fax or mail from another provider's office.

pp.05-PR.05
b. [Entity] cannot guarantee the truth, accuracy or completeness of such information. However, [Entity] will supplement, correct and validate the data upon provider notice of potential error(s).

pp.05-PR.05
b. [Entity] cannot guarantee the truth, accuracy or completeness of such information. However, [Entity] will supplement, correct and validate the data upon provider notice of potential error(s).

ph.06-PR.05
7.3. Measures to Assure Accuracy of Data. The Data Provider's obligations to provide accurate, complete and timely information.

ph.06-PR.05
The Model assumes that the Common Framework Policies and Procedures will establish minimum standards for Data Providers' obligations to provide accurate, complete, and timely information.

ph.06-PR.05
7.3.1. Applicable Common Framework Policies and Procedures. The Data Provider's obligations to comply with the applicable provisions of the Common Framework Policies and Procedures. Each Data Provider shall, in accordance with the Common Framework Policies and Procedures, use reasonable and appropriate efforts to assure that all data it provides to the System is accurate, free from serious error, reasonably complete, and provided in a timely manner.

ph.06-PR.05
7.3.2 [SNO Name] Requirements. The SNO may adopt additional requirements regarding the accuracy of data. Without limiting Section 7.3.1 (Applicable Common Framework Policies and Procedures), each Data Provider shall comply with the following requirements respecting the accuracy, completeness and timeliness of the data it provides: [insert specific description].

ph.06-PR.05
The SNO's own measures may include, for example, requiring Data Providers to adopt benchmark practices for increasing and maintaining data quality and/or requiring Participants to conduct a data quality assessment and improvement project either before or after becoming a Participant.

SP.06-PR.05
The User represents, and in furnishing the data file(s) specified in section 7 CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

The User represents further that the facts and statements made in any study or research protocol or project plan submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plans, as have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 7 will be put.

sp.02-PR.05
b. The Participant will cooperate with the [Program] Management Committee in resolving any problems with Participant Information, including an annual information audit at the Participant's offices at the [Program] Management Committee's reasonable discretion.

sp.02-PR.05
The inclusion of false, inaccurate or incomplete information may therefore cause errors affecting plans, health care quality and/or research findings.. In order to prevent such errors, the Participant, for itself and for its associated Individual Providers, if applicable, shall use its best efforts to ensure that the Participant Information submitted to the [Program] Registry by it or on its behalf, and information contained in the [Program] Registry which is reviewed by the Participant or on the Participant's behalf, is true, accurate and complete.

sp.02-PR.05
c. The [Program] Management Committee and [Entity] cannot and do not guarantee the truth, accuracy, or completeness of any information provided under this Agreement but

shall use reasonable efforts to ensure the integrity of the information received, processed and disclosed through the [Program] Registry.

mm.10-PR.05
Information Integrity

The integrity of the data shall be checked in order to detect corruption of data during transfer between the domains. The rules and techniques for this shall be agreed upon and specified in the Policy Agreement.

mm.09-PR.05
2. Trade-related Implications—Recognizing the important trade-related implications of foodborne outbreaks, epidemiologic conclusions need to be based on highly reliable scientific methods providing results which are shared with counterpart agencies in the other country.

sp.08-PR.05
The undersigned has read, understands and agrees to abide by this [Immunization] Registry Security and Confidentiality Agreement and understands other participating providers will have access to data entered into the [Immunization] Registry as outlined within this document.

PR.06 Timely Provision of Data

ph.06-PR.06
7.3.2 [SNO Name] Requirements. The SNO may adopt additional requirements regarding the accuracy of data. Without limiting Section 7.3.1 (Applicable Common Framework Policies and Procedures), each Data Provider shall comply with the following requirements respecting the accuracy, completeness and timeliness of the data it provides: [insert specific description].

ph.06-PR.06
7.3.1. Applicable Common Framework Policies and Procedures. The Data Provider's obligations to comply with the applicable provisions of the Common Framework Policies and Procedures. Each Data Provider shall, in accordance with the Common Framework Policies and Procedures, use reasonable and appropriate efforts to assure that all data it provides to the System is accurate, free from serious error, reasonably complete, and provided in a timely manner.

pp.05-PR.06
3. [Entity] will use its best efforts to make [Entity]'s system and/or the [Name] Profile system available to the Provider in accordance with the Information Services provisions of Appendix A. The Provider will access such systems according to the processes and procedures set forth in the User's Manual.

pp.05-PR.06
3. [Entity] will use its best efforts to effect the exchange of data with the Provider within 15 days after receipt of the Provider's Immunization Data.

pp.05-PR.06
C. Information to be Provided by [Entity]:

1. The Immunization Information shall be made available to the Insurer under the terms of this Agreement, under procedures and schedules to be determined by mutual agreement of the parties.

mm.09-PR.06
When do you expect to share the particular data relative to the close of the study (e.g., within N months after the close of the study to allow for data validation, immediately upon publication of the study which is expected to occur within N months of the close of the study, immediately upon submittal of a patent application which is expected to occur no later that N months after the close of the study), and by approximately what actual date would you expect the data to be shared? Who will be responsible for releasing the information?

mm.09-PR.06
2.2. Timely Sharing of Information

The value of epidemiologic information is closely linked to its timeliness. When needed, the sharing of such information between the U.S. and Mexico should occur in a time frame which allows the other country to respond to the specific health need in as timely a manner as possible, maximizing the potential for effective public health action to prevent avoidable disease, disability and mortality. As such, information shared may be preliminary in nature and subject to change as events evolve. Preliminary information should be clearly communicated as such, and should not be disseminated outside the purview of relevant public health authorities unless by mutual agreement.

mm.09-PR.06
2. Notification of Binational Cases—Recognizing that binational cases, by definition, imply a public health risk to the neighboring country and usually require prompt public health action, binational cases of notifiable infectious diseases should be promptly reported to the appropriate public health official(s) in the neighboring country. Public health authorities of both countries will need to become familiar with the list of conditions which are notifiable in each country.

mm.09-PR.06
4. Timely Reporting of Binational Cases—Time frames need to be agreed upon by both countries for reporting binational case to public health authorities. Urgently notifiable conditions should be reported within 24 hours of first identification.

mm.09-PR.06
2. Communication of Suspected Incident—Suspicion of any intentional health incident which presents a risk to citizens of the other country is to be urgently communicated to the counterpart agency responsible for such emergencies.

mm.09-PR.06
3. Ongoing Information Exchange—As such an incident evolves, information should be regularly exchanged at commonly decided intervals between corresponding public health emergency program units of both countries.

mm.09-PR.06
5. Reporting of Laboratory Results—Laboratory results are to be communicated promptly to the requesting public health agency on a confidential basis. Only the agency submitting specimens for testing is authorized to publicly communicate the findings. When appropriate, specific protocols may be agreed upon which dictate alternate procedures.

mm.09-PR.06
5.5 Public Health Communications

As expressed throughout this document, successful binational exchange of epidemiologic information for public health depends on timely and clear communication of accurate information between appropriate public health authorities of the U.S. and Mexico. Failure to do so can result not only in an inadequate public health response to prevent and control disease among binational populations, but also to misunderstandings between officials and the populations of both countries. Such misunderstandings can undermine mutual trust and confidence and can create distorted and unequal perceptions of the epidemiologic situation affecting the two countries. For these reasons, establishing clear mechanisms and protocols for public health communications between the two countries is paramount.

sp.08-PR.06
Clinic is responsible for entering immunization information into the [IIS]. It is strongly recommended that data be entered daily.

s0.08-PR.06
The inventory report generated by [IIS] for Clinic should match its actual inventory. State will conduct an annual audit at Clinic. The audit will include a verification of vaccine inventory generated by the [IIS] application to the actual doses in inventory. If inventory cannot be verified, State will work with Clinic to determine the error source and help rectify the inventory.

PR.07 Completeness of Data

pp.05-PR.07
a. [Entity] cannot guarantee that information concerning any specific individual will be available. However, [Entity] will use its best efforts to promote the entry of data into the system, in order to maintain and expand the system's coverage of the population.

ph.06-PR.07
7.3.1. Applicable Common Framework Policies and Procedures. The Data Provider's obligations to comply with the applicable provisions of the Common Framework Policies and Procedures. Each Data Provider shall, in accordance with the Common Framework Policies and Procedures, use reasonable and appropriate efforts to assure that all data it provides to the System is accurate, free from serious error, reasonably complete, and provided in a timely manner.

ph.06-PR.07
7.3.2 [SNO Name] Requirements. The SNO may adopt additional requirements regarding the accuracy of data. Without limiting Section 7.3.1 (Applicable Common Framework Policies and Procedures), each Data Provider shall comply with the following requirements respecting the accuracy, completeness and timeliness of the data it provides: [insert specific description].

sp.02-PR.07
d. The [Program] Management Committee may elect to compare the Participant Information submitted by or on behalf of the Participant against administrative data from a reliable external source (e.g., UB-92 data). If such review discloses that the Participant has reported information pertaining to substantially fewer than one hundred percent (100%) of cases required to be submitted under this Agreement, the [Program] Management Committee may decline to include information from the Participant in the [Program]

Registry and/or provide reports on procedures performed by or on behalf of the Participant, until such time as a complete record of all cases required to be submitted has been provided to the [Program] Registry by the Participant.

2. Authorized Uses and Disclosures of Participant Information.

hh.06-PR.07
d. If an Authorized User receives a request to restrict the access, use, or disclosure of patient information regarding treatment that was provided by another provider (but not including requests forwarded from another Authorized User notifying of a restriction), the Authorized User will forward that request to the treating provider and the treating provider shall be responsible for responding to the request for restrictions.

mm.09-PR.07
2.3. Quality of Information

The value of the epidemiologic information being shared depends on its accuracy and completeness. The national and state public health authorities of both countries need to commit to providing the most comprehensive and current epidemiologic information available.

PR.08 Grant of Right/License to the HIE (and its users) to Access the Data Provided; including Limitations on Use

ph.06-PR.08
5.2 Certification of Authorized Users. How the Participant will provide assurances that its Authorized Users have been trained appropriately. At the time that Participant identifies an Authorized User to [SNO Name] pursuant to Section 5.1 (Identification of Authorized Users), Participant shall certify to [SNO Name] that the Authorized User: (a) Has completed a training program conducted by Participant in accordance with Section 10.5 (Training); (b) Will be permitted by Participant to use the Services and the System only as reasonably necessary for the performance of Participant's activities as the Participant Type under which Participant is registered with [SNO Name] pursuant to Section 4.3.2 (Participant Type); (c) Has agreed not to disclose to any other person any passwords [and/or other security measures] issued to the Authorized User pursuant to Section 5.3 (Passwords and Other Security Mechanisms); (d) Has acknowledged [in writing] that his or her failure to comply with the Terms and Conditions may result in the withdrawal of privileges to use the Services and the System and may constitute cause for disciplinary action by Participant; and (e) [Others, if desired].

ph.06-PR.08
Authorized Users. Terms that govern use of the services by the Participant's Authorized Users. The Model assumes that user agreements will not be required of every individual who uses the SNO's System or Services. Instead, Participants will be responsible for designating the individuals within their organizations who would be authorized to use the SNO's System and Services ("Authorized Users").

5.1 Identification of Authorized Users. How the Participant will designate individuals who will access the SNO's System and/or use the SNO's Services. Each Participant shall provide [SNO Name] with a list in a medium and format approved by [SNO Name] identifying all the Participant's Authorized Users, together with the information described in Schedule 5 (Required Information for Authorized Users), to enable [SNO Name] to establish a unique identifier for each Authorized User. The Participant shall update such list whenever an Authorized User is added or removed by reason of termination of employment or otherwise.

ph.06-PR.08
The Model assumes that the Participant will be permitted to select its Authorized Users without review or approval by the SNO. The SNO may, however, wish to adopt specific credentialing criteria for Authorized Users that would be administered by the SNO, and which may, if desired, be set forth in the SNO Terms and Conditions. The Model assumes that Participants will be required to inform the SNO of changes to their lists of Authorized Users on an ongoing basis. This provision is likely to vary from one SNO to another, depending upon how each SNO decides to allocate responsibilities between the SNO and Participants regarding the administration of Authorized Users.

ph.06-PR.08
5.4 No Use by Other than Authorized Users. A requirement that the SNO’s System and Services be accessed and used only by Authorized Users. The Participant shall restrict access to the System and, if applicable, use of the Services, only to the Authorized Users the Participant has identified to [SNO Name] in accordance with Section 5.1 (Identification of Authorized Users).

SP.09-PR.08
Facilitate approval across the institution of data sharing arrangements via the [State] infrastructure.

ph.06-PR.08
[State Organization] hereby authorizes Provider to have access to the Network and the Databases accessible through the Network for the following uses and purposes:

A. Treatment of a patient of or by Provider.

ph.06-PR.08
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network to have access to his or her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.
- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-PR.08
1. [State Organization] may use and disclose PHI if necessary for proper management and administration of [State Organization] or to carry out the legal responsibilities of [State Organization].

ph.09-PR.08
7.5 Limitations on Use of Patient Data. Limitations the SNO will impose upon the uses of information provided by Data Providers, including uses prohibited by the Common Framework Policies and Procedures, state or local laws and regulations specific to the SNO, and other prohibitions the SNO determines are appropriate (but not in conflict with the Common Framework Policies and Procedures).

Software and/or Hardware Provided by SNO. The Model assumes that the SNO will provide certain software and/or hardware Participants would use to access the System ("Associated Software and/or Hardware"). If the SNO does not provide software and/or hardware to Participants, this section would be omitted.

8.1 Description. A description of any software and/or hardware that the SNO will provide to Participants.

8.2 Grant of License. A description of the Participant's right to use the Associated Software and/or Hardware.

8.3 Copying. Restrictions upon the Participant's right to copy software provided by the SNO.

8.4 Third-Party Software, Hardware and/or Services. How the SNO and Participants will address requirements imposed by third-party software, hardware, and/or service vendors.

9. Protected Health Information. Provisions addressing compliance with applicable laws addressing the confidentiality, security and use of patient health information.

9.1 Compliance with Policies and Procedures. Provisions requiring compliance with the Common Framework Policies and Procedures.

9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security and use laws imposed at the state and/or local level and/or other requirements that the SNO otherwise determines are appropriate (but not inconsistent with the Common Framework Policies and Procedures).

9.3 Business Associate Agreement. Provisions addressing the SNO's potential role as a business associate of the Participant.

10. Other Obligations of Participants. Additional terms governing the conduct of Participants.

10.1 Compliance with Laws and Regulations. The Participant's obligations to comply with applicable laws and regulations, generally.

mm.06-PR.08
Exchange will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

mm.06-PR.08
Exchange will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network member hospital's information system. Each Network member hospital shall maintain patient information on its information system for at least two years following a patient's discharge. If a Network member hospital archives

certain patient data, Exchange shall access the archived data in the order specified by the hospital.

mm.06-PR.08
Exchange will allow Authorized Users to access draft reports of patient information that are not yet approved and signed by a physician. The status of these reports will be designated the same in Exchange as each Network member hospital's legacy system designates the status. It is recognized that physicians in some member hospitals cannot electronically sign the drafts, and accordingly those reports will always be designated as something other than "final" or "signed."

ph.06-PR.08
Access to Specific Information and Providers. [State Organization] recognizes that certain categories of information, including but not limited to HIV status, mental health records and substance abuse records, may be more sensitive and may be accorded extra protections under state and federal law. Accordingly, as technology permits, [State Organization] will allow Patient to limit access to specific categories of information or specific providers as they see fit.

ph.06-PR.08
Provider hereby authorizes [State Organization] (and all persons participating in the [State Organization] Network) to have access to its data bases and PHI for the following uses and purposes: Treatment of a patient.

ph.06-PR.08
Mitigation of a breach of confidentiality (as defined in the [State Organization] Breach of Confidentiality Policy) or unauthorized access of PHI. Auditing and monitoring compliance with the terms and conditions of this Agreement.

ph.06-PR.08
A. Provider authorizes [State Organization] and the Network to obtain Provider's data in a mutually agreed upon format.

ph.06-PR.08
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-PR.08
7.1.1 Grant by [SNO Name]. The SNO's grant of a license to use the SNO System. [SNO Name] grants to each Data Provider, and each Data Provider shall be deemed to have accepted, a non-exclusive, personal, nontransferable, limited right to have access to and to use the System for the purposes of complying with the obligations described in this Section 7 (Data Provider's Obligations), subject to the Data Provider's full compliance with the Terms and Conditions and the Data Provider's Registration Agreement. [SNO Name] retains

all other rights to the System and all the components thereof. No Data Provider shall obtain any rights to the System except for the limited rights to use the System expressly granted by the Terms and Conditions.

ph.06-PR.08
The Model uses the legal term "license" to describe the specific rights to be granted to each Data Provider. The Model generally restricts the Data Provider's rights to access the SNO's System to those necessary to provide data in accordance with Section 7.2 (Provision of Data).

ph.06-PR.08
7.4 License. The Data Provider's agreement that the data it provides will be available for use through the Network. Subject to Section 7.5 (Limitations on Use of Patient Data), the Data Provider grants to [SNO Name] a perpetual, fully paid, worldwide, non-exclusive, royalty-free right and license (i) to license and/or otherwise permit others to access through the System and/or the NHIN and use all Patient Data provided by the Data Provider in accordance with the Common Framework Policies and Procedures and the Terms and Conditions, and (ii) to use such Patient Data to carry out [SNO Name]'s duties under the Common Framework Policies and Procedures and the Terms and Conditions, including without limitation system administration, testing, problem identification and resolution, management of the System, data aggregation activities as permitted by applicable state and federal laws and regulations, including without limitation, those promulgated under HIPAA, and otherwise as [SNO Name] determines is necessary and appropriate to comply with and carry out its obligations under all applicable federal, state, and local laws and regulations.

ph.06-PR.08
7.5 Limitations on Use of Patient Data. Limitations the SNO may impose upon the uses of information provided by Data Providers. Notwithstanding Section 7.4 (License), Patient Data provided by a Data Provider shall not be used for any of the following purposes:

ph.06-PR.08
7.5.1. Uses Prohibited by Policies and Procedures. The provisions of the Common Framework Policies and Procedures that apply to the use of information provided by Data Providers. Any use that is prohibited by the Common Framework Policies and Procedures.

ph.06-PR.08
7.5.2. Uses Prohibited by Law. Restrictions imposed by laws that are specific to the SNO, e.g., state and/or local laws. Any use that is prohibited by the laws of the State of ____________. Without limiting the generality of the foregoing, the Data Provider shall comply with the following: [list of state or local legal requirements, if desired].

ph.06-PR.08
Additional prohibitions, if desired, such as: 7.5.3. Comparative Studies. The performance of comparisons of the performance of other Participants and/or Authorized Users without the express written consent of [SNO Name] and each of the Participants and Authorized Users being compared.

sp.02-PR.08
1. The Participant's Obligation to Supply Information.

a. The Participant will submit the following information to the [Program] Registry ("Participant Information"):

(i) Data for one hundred percent (100%) of coronary artery bypass graft surgery and/or interventional cardiac catheterization performed by the Participant or, where applicable, by Individual Providers associated with the Participant in the State of [State] and such other applicable jurisdictions as may be determined by the [Program] Management Committee, beginning on the effective date of this Agreement and continuously as such data is received by the Participant until this Agreement is terminated.
(ii) Notice of any potentially erroneous and/or missing data with respect to cases previously reported by or on behalf of the Participant.
(iii) Corrected or corroborating data in the event the [Program] Management Committee or the Participant has reason to believe any information submitted to and/or contained in the [Program] Registry is not true, accurate, or complete.

sp.02-PR.08
c. The Participant hereby acknowledges that Participant Information submitted to and/or contained in the [Program] Registry may be relied upon for purposes of planning, quality assessment and improvement, and research.

ph.05-PR.08
Under no circumstances shall The Regents be required under this Agreement to provide the User with any information that does not qualify as part of a "limited data set" under 45 C.F.R. § 164.514(e).

hh.06-PR.08
Except as expressly set forth in this Agreement, neither Network will obtain any rights in the other's Exchange, Documentation, any of the technology used to create the other's Exchange, including electronic formats and tools that the Network or Authorized User uses in interfacing the Data into the Exchange, or in all related software, hardware, documentation, and methodologies used by the other Network, or its Authorized Users, to develop, maintain, and operate the Exchange and deliver services to a Network.

hh.06-PR.08
Each Authorized User shall agree to an Exchange Agreement detailing the permitted uses of the system, HIPAA compliance requirements and the user's roles and responsibilities. Each Authorized User's consent to the agreement will be logged in an audit trail or otherwise documented.

The enrolling Network immediately shall remove an Authorized User's or Registered User's access to the Exchange if the user no longer qualifies as an Authorized User or Registered User.

mm.06-PR.08
Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient's data through Exchange. If a patient has chosen this option, when a query is made about that particular patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details." If a patient desires to revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

mm.06-PR.08
Exchange will not allow any Authorized User access to any patient information from a dedicated acute in-patient or outpatient psychiatric unit or an in-patient or outpatient substance abuse facility, as designated by each Network member hospital. Each hospital shall have the right to exclude from Exchange non-hospital patient data that is contained within its clinical information system.

mm.06-PR.08
Exchange will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

mm.06-PR.08
Exchange will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network member hospital's information system. Each Network member hospital shall maintain patient information on its information system for at least two years following a patient's discharge. If a Network member hospital archives certain patient data, Exchange shall access the archived data in the order specified by the hospital.

mm.06-PR.08
Exchange will allow Authorized Users to access draft reports of patient information that are not yet approved and signed by a physician. The status of these reports will be designated the same in Exchange as each Network member hospital's legacy system designates the status. It is recognized that physicians in some member hospitals cannot electronically sign the drafts, and accordingly those reports will always be designated as something other than "final" or "signed."

PR.09 Compliance with Applicable Law

ph.06-PR.09
7.5.2. Uses Prohibited by Law. Restrictions imposed by laws that are specific to the SNO, e.g., state and/or local laws. Any use that is prohibited by the laws of the State of [Insert State Here]. Without limiting the generality of the foregoing, the Data Provider shall comply with the following: [list of state or local legal requirements, if desired].

ph.06-PR.09
7.4 License. The Data Provider's agreement that the data it provides will be available for use through the Network. Subject to Section 7.5 (Limitations on Use of Patient Data), the Data Provider grants to [SNO Name] a perpetual, fully paid, worldwide, non-exclusive, royalty-free right and license (i) to license and/or otherwise permit others to access through the System and/or the NHIN and use all Patient Data provided by the Data Provider in accordance with the Common Framework Policies and Procedures and the Terms and Conditions, and (ii) to use such Patient Data to carry out [SNO Name]'s duties under the Common Framework Policies and Procedures and the Terms and Conditions, including without limitation system administration, testing, problem identification and resolution, management of the System, data aggregation activities as permitted by applicable state and federal laws and regulations, including without limitation, those promulgated under HIPAA, and otherwise as [SNO Name] determines is necessary and appropriate to comply with and carry out its obligations under all applicable federal, state, and local laws and regulations.

ph.06-PR.09
Providing customized summary reports with non-identifying data or statistics as needed for public health or other governmental purposes required by law.

ph.06-PR.09
XI. Effect of Governmental Laws and Regulation

Each party shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally funded healthcare program, including the Medicare and Medicaid programs.

ph.06-PR.09
Access to Specific Information and Providers. [State Organization] recognizes that certain categories of information, including but not limited to HIV status, mental health records and substance abuse records, may be more sensitive and may be accorded extra protections under state and federal law. Accordingly, as technology permits, [State Organization] will allow Patient to limit access to specific categories of information or specific providers as they see fit.

ph.06-PR.09
Providing customized summary reports with non-identifying data or statistics as needed for public health or other governmental purposes required by law.

ph.06-PR.09
Compliance with Law. [State Organization] shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which [State Organization] reasonably believes: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally-funded healthcare program, including the Medicare and Medicaid programs.

mm.10-PR.09
Health care personnel who hold licenses, certificates or other permits issued by a sending signatory as evidence of qualification to provide professional, mechanical or other services will be deemed licensed, certified, permitted and competent to provide those services within the jurisdiction of any receiving signatory requesting their services in preventing, detecting or responding to a public health emergency. Such health care personnel shall not be subject to civil, criminal or regulatory process within the jurisdiction of the sending or receiving signatory on the grounds that they have engaged in the unqualified or unauthorized practice of their regulated service. This section also applies to operators of emergency vehicles engaged in transporting evacuees and/or refugees as contemplated in Section V.A.

ph.06-PR.09
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network) to have access to his/her PHI for the following uses and purposes:

Treatment of patient. Mitigation of a breach of confidentiality or unauthorized access of PHI.

Payment for healthcare services. Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.

Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-PR.09
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-PR.09
9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security, and use laws imposed at the state and/or local level. [SNO Name] and each Participant shall comply with the requirements for the privacy, security, and use of patient health information imposed under the laws of the State of [Insert State here]. Without limiting the generality of the foregoing, [SNO Name] and each Participant shall comply with the following: [list of state or local legal requirements, if desired].

ph.06-PR.09
10.1 Compliance with Laws and Regulations. The Participant's obligations to comply with applicable laws and regulations, generally. Without limiting any other provision of the Terms and Conditions relating to the parties' compliance with applicable laws and regulations, the Participants shall perform in all respects as contemplated by the Terms and Conditions, in compliance with applicable federal, state, and local laws, ordinances and regulations.

ss.05-PR.09
As designated by the joint working group, each signatory should provide copies of their respective statutes or regulations related to public health events, infectious disease agents and other relevant material as needed to every other signatory. Each signatory should ensure that the copies so provided are accurate and current, The signatories should jointly identify and maintain in common a set of materials, which they agree reflect the applicable laws and regulations of the Governments of the United States and Canada.

ss.05-PR.09
Nothing in this Agreement is to be construed so as to require any signatory to transmit health data in contravention of the law under which the sending signatory is bound.

mm.09-PR.09
2.7. Respect for the Sovereignty and Laws of Each Country

The responsibility for all public health responses to binational epidemiologic events lies with the public health agencies of the country where the respective activities will take place. All parties recognize the need for these same public health agencies to operate within the legal framework established by that country. If legal barriers are identified which limit the capacity of public health agencies to collaborate with counterpart agencies of the other country in the most effective way, such barriers should be addressed by the appropriate authorities with the objective of maximizing the benefit to the public's health in each country.

mm.09-PR.09
1. Regulatory Responsibilities in Foodborne Disease Outbreaks—Given that tracebacks and product recalls resulting from foodborne disease outbreaks fall under the legal responsibility of regulatory agencies, sharing of information needs to be conducted in accordance with the duties of those agencies and within the framework of the existing agreements between the food regulatory agencies in Mexico and the United States.

sp.04-PR.09
C. Other Provisions:
Disputes: This Agreement is subject to the laws of the State of [State]." Any dispute arising from the terms and conditions of this Agreement, which cannot be resolved by mutual agreement, will be tried in Circuit Court, [County], [State].

PR.10 Obligation to Obtain and Maintain Compliant Software/Hardware Necessary to Utilize the HIE

ph.06-PR.10
10.3 Software and Hardware Provided by Participant. Provision requiring the Participant to obtain and maintain all hardware and software required to use the System and the Services that is not to be provided by the SNO. Each Participant shall be responsible for procuring all equipment and software necessary for it to access the System, use the Services (including the Associated Software), and provide to [SNO Name] all information required to be provided by the Participant ("Participant's Required Hardware and Software"). Each Participant's Required Hardware and Software shall conform to [SNO Name]'s then-current specifications. [SNO Name] may change such specifications from time to time in its sole discretion upon not less than sixty (60) days prior notice to each Participant affected by the change. As part of the Participant's obligation to provide Participant's Required Hardware and Software, the Participant shall be responsible for ensuring that all the Participant's computers to be used to interface with the System are properly configured, including but not limited to the operating system, web browser, and Internet connectivity.

ph.06-PR.10
The Model assumes that the SNO will provide some of the software and hardware that Participants will require to use the System, as described in Section 8 (Software and Hardware Provided by [SNO Name]), and that the Participant will be required to provide the remainder (e.g., a personal computer with an operating system and web browser meeting certain specifications), as described in Section 10.3 (Software and/or Hardware Provided by Participant). The terms of Section 8 (Software and/or Hardware Provided by [SNO Name]) and Section 10.3 (Software and Hardware Provided by Participant) should be revised as necessary to conform to each other.

ph.06-PR.10
10.4 Malicious Software, Viruses, and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO's System. The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including without limitation the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine, or data (including without limitation malicious software or "malware," viruses, worms, and Trojan Horses) which will disrupt the proper operation of the System or any part thereof or any hardware or software used by [SNO Name] in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by [SNO Name] or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

mm.06-PR.10
Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient's data through Exchange. If a patient has chosen this option, when a query is made about that particular patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details". If a patient desires to revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

sp.08-PR.10
Clinic may use the computer for other applications when [IIS] is not in use. [IIS] must be given top priority. Periodic software upgrades of [IIS] will be performed by State personnel. While every effort will be made to not adversely impact other applications Clinic has installed, resolution of non-[IIS] problems is ultimately Clinic's responsibility.

PR.11 Training of Employees/Agents

ph.06-PR.11
10.5 Training. A description of the training, if any, that the SNO will require the Participant to provide to its personnel. The Participant shall provide appropriate and adequate training to all of the Participant's personnel, including without limitation Authorized Users, in the requirements of applicable laws and regulations governing the confidentiality, privacy, and security of protected health information, including without limitation requirements imposed under HIPAA.

mm.07-PR.11
a. Prior to receiving a passcode or other necessary tools for accessing [State Organization], a person must have both their identity and authority verified in accordance with the procedures described below.

b. The following forms of identification are sufficient for verifying a person's identity:

- Official and valid state ID (driver's license, state ID card);
- Official and valid federal ID (passport, military or government ID); or
- Official and valid entity-issued picture ID.

c. The following items are sufficient for verifying a person's authorization to access [State Organization]:

Entity-issued ID indicating authorization to access [State Organization];
Authorization on official entity letterhead from the Privacy Officer or other person designated to determine access levels for [State Organization]; or
E-mail authorization from the official entity email address of the Privacy Officer or other person designated to determine access levels for [State Organization].

d. If a person provides sufficient documentation to meet the requirements of subsections (b) and (c) above, a passcode or other necessary tools for accessing [State Organization] may be issued. At the time of issuance, the person supplying the passcode or other necessary tools should place a copy of the identification and authorization documents in the designated [State Organization] Verification File.

e. If a person provides any other type of identification or authorization (student ID, court order, etc.), please contact the Privacy Officer or other person designated by this entity to determine access levels for [State Organization].

f. The majority of persons requiring access to [State Organization] should have their identification and authorization verified prior to any necessary use of the system. For this reason, emergency access to [State Organization] should not be necessary. If, however, a person requests emergency access, the entity should contact an on call provider with access to the system to assess the totality of the situation on a reasonableness basis.

ph.06-PR.11
Provider agrees to be bound by the policies and procedures of [State Organization], as may be amended from time to time by [State Organization]. The policies and procedures of [State Organization] shall be considered a part of this Agreement. Provider agrees to review these policies and procedures with employees and to obtain an attestation of such policies and procedures from each employee prior to providing access to the Network.

mm.07-PR.11
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers may also be required to provide [State Organization] with a list of active staff members with access to [State Organization], in accordance with the Provider Participation Agreement. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

pp.06-PR.11
That such designated personnel have received training regarding the confidentiality of PHI under the Privacy Rule and all other applicable State and local laws and agree to protect the Information in compliance with the Privacy Rule, such laws and this Agreement

ph.06-PR.11
Provider agrees to supply [State Organization] with the names of any persons who are given access to the Network, and a quarterly list of the active staff with access to the Network (due by the 15th of January, April, July and October). Provider should be aware, and should make potential employees aware, that individuals may be denied access to the Network based on past performance or behavior reported by a former employer or other participating provider.

mm.04-PR.11
Identification and Limitation of Personnel Entitled to Access

mm.09-PR.11
2.4. Communication Pathways

Clearly defined pathways between public health agencies of the US and Mexico for communication of such epidemiologic information are needed to ensure rapid delivery to the appropriate agency and a high potential for action based on the information. When a specific need for binational information exchange arises, public health agencies at the local, state or federal levels of one country should communicate with their counterpart agency of the same level in the other country (i.e., local-local, state-state, or federal-federal). This should be conducted in parallel with communication to national partners, as defined by national policies. Communication to other levels of government (local-state, state-federal) is the responsibility of the agencies of each country, not of agencies in the neighboring country. Thus, once an agency in the second country is notified of an epidemiologic event, the responsibility lies with that same agency to notify partner public health agencies of the same country, unless specific guidelines dictate otherwise. While communications transmitted in the language of the other country are encouraged, those receiving communications should be sufficiently fluent in the language of the other country to understand messages composed in that language.

mm.09-PR.11
6. Binational Laboratory Collaboration—Collaborative activities between cross-border laboratories is encouraged to enhance the scope of diagnostic capabilities available and the quality of the services provided. This may include training, provision of equipment, supplies and/or reagents, and participation in quality assurance programs. As with cross-border transport of specimens, agreements between public health agencies and customs authorities should be established to define protocols which facilitate the passage of such material. Roles of national and state public health agencies for coordination of such activities need to be defined by each country.

hh.06-PR.11
3.4 Authorized User Training. Networks shall assure by contract or otherwise that Authorized Users who are granted Data User Accounts have education and training for Registered Users on HIPAA requirements to maintain the confidentiality of patient information accessed through the Exchanges.

sp.08-PR.11
The [Immunization] Registry Security and Confidentiality Agreement must be signed by a representative of the participating health care entity or school, prior to any training on use of the [Immunization] Registry and gaining access to the Registry data. One or more persons from each site must complete the training for the [Immunization] Registry Site Administrator(s). Having completed the training, the Site Administrator(s) may enroll users who have been trained in the use of the [Immunization] Registry at the appropriate access level and have signed the [Immunization] Registry User Security and Confidentiality Agreement. The [Immunization] Registry Coordinator will maintain a file of signed [Immunization] Registry User Security and Confidentiality Agreements and will require new agreements to be signed by users every two years. The participating health care entity or school assumes responsibility for the individual’s usage of the [Immunization] Registry. Providing access to [Immunization] Registry to outside organizations is strictly forbidden.

sp.08-PR.11
The [IIS] project team, consisting of State and contract personnel, is responsible for Clinic's initial [IIS] application training. This training is not intended to provide basic personal computer, Windows, or browser skills, which are Clinic's responsibility. State will provide additional training as changes to the application merit. State is responsible for providing a copy of routine updates and the [IIS] application User's Guide to Clinic.

PR.12 Miscellaneous Provider Requirements Provisions

pp.06-PR.12
Section 3.01 Storage of Information on the Network. The Participants shall store Information in electronic data files dedicated to each respective Participant on the Network. The Participants agree that they each shall make good faith efforts to store, at a minimum, the following information:

4. Permitted Uses and Disclosures of Data.

ph.02-PR.12
a. PROVIDER/REPOSITORY may use data owned by the Data Provider to create limited data sets including the elements set forth in Appendix A, and may disclose such limited data sets to RESEARCHER or its authorized contractors subject to this Agreement.

pp.06-PR.12
For Participants with emergency departments, encounter information for each emergency department visit, and for Participants with primary care or hospital visits, encounter information for such visits. Encounter information shall include: patient demographic information, reason for visit, treating health care provider(s), date of visit, place of visit, diagnoses, and procedures.

pp.06-PR.12
Vital signs, pathology reports, radiology studies and images, discharge summaries, operative notes, inpatient medications, laboratory test results, cardiology studies, and other diagnostic tests to the extent that Participants have the capability to submit such information electronically.

Participants may store Information in addition to the minimum set of Information required by this Paragraph and are encouraged to submit any and all information that may be relevant to the clinical care of a patient. The Management Committee may not vote to reduce the Information to be submitted to the Network defined in this Agreement. Notwithstanding any of the foregoing, Participants shall not be required to submit any information that is protected from disclosure by 42 C.F.R. Part 2 (alcohol and drug abuse patient records that are maintained in connection with the performance of any federally assisted alcohol and drug abuse program), and shall not submit psychotherapy notes as that term is defined by 45 C.F.R. § 164.501.

pp.06-PR.12
Section 3.02 Participants' Representation Regarding Legality of Storage. To the best of each Participant's knowledge, storing the Information on the Network does not violate any rights, including copyrights, of third parties.

pp.06-PR.12
Section 4.01 Participant Access for Treatment.

(a) Subject to the conditions set forth below, when a patient is under the Treatment of a Full Participant, all other Full Participants shall grant the treating Participant (and the individuals the treating Participant designates pursuant to Section 4.04) full access to the Information stored on the Network for purposes of treating the patient.

As approved by the individual Participants and pursuant to any separate agreement between such Participants and [Organization] (either directly or as a subcontractor with another non-profit community organization), [Organization] may transmit or deliver reports (including, but not limited to, face sheets, laboratory results, radiology reports, and dictated notes) to health care providers with whom the Participants have an agreement or obligation to provide such reports. The financial terms and other details of such transmissions or deliveries shall be governed by the respective separate agreements.

pp.06-PR.12
Section 4.02 Participant Access for Other Purposes. Subject to a reasonable retrieval fee to be determined by [Organization], each Participant will have access to the Information it stores on the Network in accordance with its own internal regulations governing access to its own internal records (provided said regulations are reasonable and adequately protect the confidentiality of the Information). The reasonable retrieval fee noted in this Section does not apply when a Full Participant seeks Information for the Treatment of a patient.

pp.06-PR.12
Section 4.03 Participants’ Representation Regarding Legality of Access. Each Participant represents and warrants that it is authorized to allow the Full Participants, [Organization], and [Organization]'s subcontractors to access the Information as set forth in this Agreement pursuant to the Privacy Rule and [State] Code §§ 16-39-5-1 and 16-39-5-3, and/or pursuant to a duly executed authorization from any Individual to whom the Information applies.

pp.06-PR.12
Section 4.04 Access to Information By Participants’ Personnel. Each Participant shall determine the personnel under its control (including any personnel of physician practice groups allowed to access Information pursuant to Section 4.01(b)) who may access the Network to retrieve Information for the Treatment of patients. For Participants who are technically able to do so, each Participant shall provide daily electronic files to [Organization] of the individuals it designates under this Section. If such electronic notice is not feasible, each Participant shall provide lists of such individuals through e-mail, hard copy, or facsimile to [Organization] no less frequently than biweekly. Each Participant shall certify:

pp.06-PR.12
(b) That such designated personnel shall only access the Network for purposes of Treatment of a patient;

pp.06-PR.12
(c) That such designated personnel have agreed to hold any passwords, or other means for accessing the Network, in a confidential manner and to release them to no other individual;

pp.06-PR.12
(d) That such designated personnel have agreed to participate in various studies that may be conducted from time to time related to various issues surrounding the Network, including, but not limited to, the efficacy and usefulness of the Network; and

pp.06-PR.12

(e) That such designated personnel agree and understand that their failure to comply with the terms of this Agreement may result in their exclusion from the Network and may constitute cause for disciplinary action by the Participant.

pp.06-PR.12

Full Participants may continue to access all Network Information pursuant to ARTICLE IV and ARTICLE V of the Agreement until such time as an election is made by a submitting Participant to disallow such access to its own Information. If a Participant elects to disallow access to its own Information on the Network, such electing Participant's Information will no longer be available to other Full Participants and such an electing Participant, if a Full Participant, shall thereafter be precluded from accessing the Network. Notwithstanding, Information may continue to be used and disclosed for the reasons described in Section 12.05.

pp.06-PR.12

Continued use and disclosure of the Information pursuant to Section 12.02(a) and Section 12.02(b) shall be subject to ARTICLE V, ARTICLE VII, ARTICLE VIII, and ARTICLE IX.

pp.06-PR.12

Section 12.04 Use and Disclosure of Information After Withdrawal.

(a) A Participant that withdraws from this Agreement, regardless of whether such withdrawal complies with Section 12.03 of this Agreement, need not continue submitting additional Information for storage on the Network. However, any Information stored on the Network at the time of the withdrawal must be left on the Network for a period of two (2) years after the termination of the Agreement, during which time [Organization] may continue to use the Information for scientific and research purposes, including, but not limited to, publication of research results in accordance with ARTICLE VII and ARTICLE VIII. After the two-year period, Participants may request that their Information no longer be used or disclosed for any purpose. Until such a request is made, [Organization] may continue to use the Information in compliance with this Section, provided [Organization] gives prior written notice to the affected Participants of any such use. Notwithstanding the foregoing, Information must continue to be stored on the Network for a longer period of time to the extent that Participants have agreed to make their Information available for research project approved pursuant to ARTICLE VII, in which case the Information shall continued to be stored, and may continue to be used and disclosed, for the duration of such research projects in compliance with the terms of the projects. After the applicable period discussed above, [Organization] shall no longer use or disclose the Information for research purposes and the provisions of ARTICLE V (Confidentiality) and ARTICLE VIII (HIPAA Business Associate Provisions) shall continue to apply to the Information.

pp.06-PR.12

Notwithstanding the foregoing Section 12.04(a), if a Participant withdraws because of a significant breach of [Organization]'s duties under ARTICLE VII or ARTICLE VIII with regard to Information stored on the Network by the withdrawing Participant, the provisions of Section 12.04(a) shall not apply and [Organization] may no longer use or disclose the Information for research purposes.

sp.07-PR.12
ss.07-PR.12

The [State] DH will periodically monitor the facility and user’s activities related to usage of the [Immunization].

mm.04-PR.12
Provisions for Mandatory Increases in Security Measures and Privacy Procedures to Meet Evolving Standards.

mm.10-PR.12
The signatories will meet and confer to establish a process and/or location for their joint communication and coordination of resources (personnel, material and information) during public health emergencies.

mm.10-PR.12
The signatories will meet and confer to establish procedures by which to share information regarding the location, distribution, transportation and maintenance of essential materials necessary for public health emergencies.

mm.10-PR.12
The signatories will meet and confer to discuss planning for the care of persons transferred at the request of co-signatories. The purpose of such discussion and planning is to offer reassurance to all signatories that each is minimally prepared to offer assistance to its neighbors should it be called upon to do so pursuant to this Annex and Agreement.

This Annex is effective upon its execution or adoption by any two or more signatories. Entry into force of this Annex is subject to the laws of the United States of America and the Government of Canada and the several signatories. The signatories shall enact such legislation as may be necessary to effectuate this Annex. Duly authenticated copies of this Annex in the English and French languages shall be deposited with each of the signatories.

This Annex is to be construed to effectuate the purposes of the Agreement. This Annex is not to be applied in derogation of any superseding law of the United States or Canada. In the event than any provision is declared unconstitutional or unlawful or held inapplicable to any person or circumstance, the signatories intend for the remainder of this Annex to continue with full force and effect.

ph.02-PR.12
2. Data Quality. The Data Provider shall have no obligation to make available any data other than that hosted by PROVIDER/REPOSITORY, or to process or take any action with respect to any data. Neither the Data Provider nor

ph.02-PR.12
Effect of Termination. Upon the termination of this Agreement for any reason:

a. PROVIDER/REPOSITORY shall stop the creation of limited data sets derived from data owned by the Data Holder, and the disclosure of such limited data sets to RESEARCHER; and

ph.02-PR.12
b. RESEARCHER and any contractor(s) shall (i) if requested by the Data Provider, return copies of all data in their possession to PROVIDER/REPOSITORY, and (ii) destroy all copies of data in their possession, including erasure or overwriting of electronic data or destruction of electronic media sufficient to render the data unrecoverable.

pp.05-PR.12
V. [Entity] shall provide the Insurer with a current and periodically updated Insurance User’s Manual, which shall describe the processes and procedures, and other

features and requirements for exchange of information through [Entity]'s Information System. The Insurance User's Manual shall be considered a part of the contractual relationship between [Entity] and the Insurer. The Insurance User's Manual may modify the terms of this Agreement, but shall under no circumstances establish processes or procedures which fail to meet all applicable individual health information privacy protection standards in force under state and federal law, and shall be updated if and when necessary to ensure such compliance.

ph.06-PR.12
Provider agrees to supply [State Organization] with the names of any persons who are given access to the Network, and a quarterly list of the active staff with access to the Network (due by the 15th of January, April, July and October). Provider should be aware, and should make potential employees aware, that individuals may be denied access to the Network based on past performance or behavior reported by a former employer or other participating provider.

pp.05-PR.12
3. [Entity] shall disclose information pertaining to identified Enrollees only to those Enrollees, to their parents or other legal guardians (if applicable), and to health care providers who have entered into a Health Care Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that Enrollee, unless (a) [Entity] is provided with a Release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-PR.12
IV. [Entity] shall provide the Provider with a current and periodically updated User's Manual, which shall describe the processes and procedures, and other features and requirements for use of the [Entity] system. The User's Manual shall be considered a part of the contractual relationship between [Entity] and the Provider for use of the [Entity] System. The User's Manual may modify the terms of this Agreement, but shall under no circumstances establish processes or procedures which fail to meet all applicable individual health information privacy protection standards in force under state and federal law, and shall be updated if and when necessary to ensure such compliance.

pp.05-PR.12
3. [Entity] shall disclose information pertaining to identified individual patients only to those individuals, their parents or other legal guardians, or health care providers who have entered into an Individual Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that patient, unless (a) [Entity] obtains a release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-PR.12
E. Information to be Provided by [Entity]:

1. The information and data access services available to the Provider under this agreement are set forth in Appendix A to this Agreement. [Entity] may make additional or enhanced Information Services available to the Provider from time to time, by giving written notice of the amendment including identification of the change, any associated costs, and any modifications to user procedures which pertain to such amendment. Such amendments will be incorporated into this agreement in the form of amendments to the Information Services, and become effective upon the Provider's receipt of the notice of amendment from [Entity]. Such amendments shall not affect the other provisions of this contract.

pp.05-PR.12
4. [Entity]’s Information Services may include recommendations for immunization treatments, information related to the vaccines used in providing immunization treatments, and other information relevant to the provision of immunization services. [Entity] will use its best efforts to ensure that all such recommendations and information is derived from recognized medical and/or pharmaceutical authorities, and is regularly updated to maintain its validity. However, the Provider is solely responsible for ensuring that independent professional judgment is used in making use of such information.

pp.05-PR.12
2) [Entity] shall provide the Provider with a current and periodically updated User’s Manual, which shall describe the processes and procedures, and other features and requirements for use of the [Entity] system. The User’s Manual shall be considered a part of the contractual relationship between [Entity] and the Provider for use of the [Entity] System. The User’s Manual may modify the terms of this Agreement, but shall under no circumstances establish processes or procedures which fail to meet the individual health information privacy protections standards which are in force under state and federal law, and shall be updated if and when necessary to ensure such compliance.

pp.05-PR.12
ii) [Entity] shall disclose information pertaining to identified individuals only to those individuals, their parents or other legal guardians, or to health care providers who have entered into an Individual Provider Information Sharing Agreement with [Entity] and who need the information in order to provide health care to that patient, unless (a) [Entity] obtains a release under the terms stated below, or (b) pursuant to a court or agency order requiring such disclosure.

pp.05-PR.12
1. The information and data access services available to the Provider under this agreement are set forth in Appendix A to this Agreement. [Entity] may make additional or enhanced Information Services available to the Provider from time to time, by giving written notice of the amendment including identification of the change, any associated costs, and any modifications to user procedures which pertain to such amendment. Such amendments will be incorporated into this agreement in the form of amendments to the Information Services, and become effective upon the Provider's receipt of the notice of amendment from [Entity]. Such amendments shall not affect the other provisions of this contract.

mm.06-PR.12
To ensure that all users of the Provider’s systems fully comply with the Security Policies and Procedures, the Provider will discipline and sanction such users, as appropriate, for any violation of the Security Policies in accordance with the following:

A. General Rule.

The Provider shall apply appropriate sanctions against any person that fails to comply with the Provider’s Security Policies and Procedures.

The type and severity of sanction applied shall be in accordance with the Provider’s Privacy and Security Policies and Procedures.

Employees, agents, and other contractors should be aware that violations of a severe nature may result in notification by [State Organization] to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.

mm.06-PR.12
B. Process for Responding to Possible Violations.

Persons affiliated with the Provider, regardless of whether they have access to [State Organization], are encouraged to report possible breaches of confidentiality to the Provider's Privacy Officer.

The Provider shall respond to possible violations in accordance with the Provider's Security Policies and Procedures and general procedures for violation of Provider policy. The name of any persons involved with the possible violation shall be reported to [State Organization] within ten (10) days of the discovery of the violation.

A record of the event and any discipline imposed shall be maintained in the employee's personnel file with a copy to be filed in a master file maintained by the Privacy Officer, and to be provided to [State Organization] within sixty (60) days of the event.

Appropriate Provider personnel are responsible for determining the severity of sanctions necessary, in accordance with Provider policies and procedures. A record of the final determination shall be maintained by Provider, to be provided to [State Organization] within sixty (60) days of the determination.

mm.06-PR.12
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

mm.06-PR.12
1. Protected Health Information in Paper Form – Provider personnel must ensure that all Provider policies and procedures regarding PHI in paper form are followed. [State Organization] does not make use of paper records and places no further restrictions on the use of paper records beyond already established Provider policies and procedures.

mm.06-PR.12
Providers who participate in [State Organization] may be asked at any time to provide evidence of compliance with this policy, and to validate that appropriate policies and procedures are in place to comply with this policy. Providers must at all times comply with the Provider Participation Agreement, including any actions taken by [State Organization] in accordance with such agreement.

ph.06-PR.12
3.1 Generally. The Terms and Conditions apply to the operation of the System, the provision of the Services, and the relationships among [SNO Name] and Participants with respect thereto.

ph.06-PR.12
3.2 Development and Dissemination; Amendments. How the SNO adopts the SNO Terms and Conditions, makes changes to the Terms and Conditions, and informs Participants of those changes. [SNO Name] is solely responsible for the development of the Terms and Conditions, and may amend, or repeal and replace, the Terms and Conditions at any time as [SNO Name] determines is appropriate. [SNO Name] generally shall notify all Participants of any changes to the Terms and Conditions at least thirty (30) days prior to the implementation of the change. However, if the change is required in order for [SNO Name]

and/or Participants to comply with applicable laws or regulations, [SNO Name] may implement the change within a shorter period of time as [SNO Name] determines is appropriate under the circumstances.

ph.06-PR.12
Because the SNO Terms and Conditions are to be incorporated into each Participant's Registration Agreement, the SNO may find it necessary to limit its ability to change certain provisions of the SNO Terms and Conditions. These limits may be described in this part of the SNO Terms and Conditions. The Model assumes that the SNO may make changes at will, but that Participants must either consent or acquiesce to changes that affect their rights or obligations (see Section 4.2 (Registration by Agreement) and Section 4.5 (Changes to Terms and Conditions)). The SNO may find that Participants or other members of the SNO's community wish to participate in the development of the Terms and Conditions, as well as participate in the decision to make changes. For this reason, the Model's discussion of the Management Committee allows for the possibility that Participants and/or others will be involved in deciding upon changes to the Terms and Conditions (see Section 11.6 (Management Committee)).

ph.06-PR.12
4.3 Online Registration. How Participants may register online.

ph.06-PR.12
4.3.2 Participant Type. How the SNO will categorize Participants by their respective roles in the health care system. Each registrant shall register to participate in one of the following Participant Types: (a) Physician or medical group; (b) Laboratory; (c) Hospital; (d) Public health agency; (e) Pharmacy; (f) Pharmacy benefit manager; (g) Health plan, insurer or other payor; (h) Researcher; and (i) [additional or different provider types selected by the SNO, subject to any limits imposed by the Common Framework Policies and Procedures].

ph.06-PR.12
4.3.3 Approval and Disapproval of Registration Forms. The SNO will be entitled to review all registration forms and decide not to accept any given party's registration. [SNO Name] shall review each Registration Form and shall approve or disapprove each in accordance with the Terms and Conditions and as [SNO Name] determines in its sole discretion is appropriate. [SNO Name] shall not be required to approve any Registration Form or other application to be a Participant.

ph.06-PR.12
The Model is drafted to provide the SNO maximum flexibility in controlling who may become a Participant. The SNO may wish to reserve the right not to register a particular Participant if, for example, the SNO determines that the person is not eligible to participate or is not expected to comply with the SNO Terms and Conditions. In addition, the SNO may wish to adopt specific credentialing criteria for Participants, which may, if desired by the SNO, be set forth in the SNO Terms and Conditions. The SNO may wish to consider whether it wishes to disclose to an unsuccessful applicant the bases upon which its application for registration was not approved.

ph.06-PR.12
5.3 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users. Based on the information provided by the Participant pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized

User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

ph.06-PR.12
5.5 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users. The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant's Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant's Authorized Users, with respect to the System, the Services and/or any confidential and/or other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant.

ph.06-PR.12
7. Data Provider's Obligations. Provisions that apply specifically to "Data Providers" (i.e., Participants registered to provide data). Provisions that apply specifically to "Data Recipients" (i.e., Participants registered to use the SNO's Services) appear at Section 6 (Data Recipient's Right to Use Services)). If the Participant is registered with [SNO Name] as a Data Provider, the terms of this Section 7 (Data Provider's Obligations) shall apply to that Participant.

ph.06-PR.12
7.2 Provision of Data. Terms that apply to the Data Provider's delivery of data to the Network, e.g., format(s), standards, etc.

ph.06-PR.12
Additional prohibitions, if desired, such as 7.5.3. Comparative Studies. The performance of comparisons of the performance of other Participants and/or Authorized Users without the express written consent of [SNO Name] and each of the Participants and Authorized Users being compared.

ph.06-PR.12
9.3 Reporting of Serious Breaches. Provisions requiring the SNO and Participant to report to each other concerning serious breaches of confidentiality of patient health information. Without limiting Section 9.4.7(Reports), if applicable to [SNO Name], [SNO Name] and Participant shall report to the other any serious use or disclosure of Protected Health Information not provided for by the Terms and Conditions of which [SNO Name] or Participant becomes aware, and any security incident concerning electronic Protected Health Information (a "Serious Breach of Confidentiality or Security"). A "Serious Breach of Confidentiality or Security" is one that adversely affects (a) the viability of the NHIN; (b) the trust among Participants or (c) the SNO's legal liability.

ph.06-PR.12
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of

breaches in security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:]

ph.06-PR.12
11.6 Management Committee.

Certain SNOs may wish to include certain terms regarding internal governance and management as a part of the SNO Terms and Conditions, to assure that Participants may be involved in their governance and/or management. The language provided here is for illustration only, and is not intended to limit how the SNO would structure its governance or Participants' involvement in governance and management. SNOs that do not desire such provisions would omit this section entirely.

ph.06-PR.12
11.6.1 Composition. [SNO Name] shall create and maintain a Management Committee (the "Management Committee") composed of [specified personnel/representatives of SNO and specified number of Participant representatives, who shall be selected in a specified manner].

ph.06-PR.12
11.6.2 Meetings and Responsibilities of Management Committee. The Management Committee shall meet [describe intervals, e.g., monthly] to consider and resolve various issues pertaining to the use of the System and the Services by Participants, including [list].

ph.06-PR.12
Issues that a Management Committee could address include, without limitation, technical issues, confidentiality, the scope of information stored and accessed by Participants, the use of the information, changes to the Terms and Conditions, and any other issues related to the network or the parties' participation therein.

ph.06-PR.12
11.6.3 Management Committee Bylaws. The Management Committee shall adopt bylaws for the conduct of its meetings and other proceedings.

ph.06-PR.12
2. Review of Application

[SNO Name] will review this application for registration and may accept or reject this application in accordance with the terms and conditions set forth in Section __ of the [SNO Name] Terms and Conditions. Upon [SNO Name]'s acceptance of this application, [SNO Name] shall notify the Applicant and shall register the Applicant as a [Participant]. [Optional, if SNO is to issue passwords:] [SNO Name] shall issue each Participant a [User I.D. and] password to access and use the [SNO Name] System and the [SNO Name] Services.

mm.09-PR.12
CONTENT OF THE DATA SHARING PLAN

I. Background of the Institution and the project that is adopting [Program] tools and using the Grid to share data

Describe the institution that is conducting the research (may be a unit or department of a larger institution):
Will any or all of the data be collected specifically for the current project?

mm.09-PR.12
Describe any sponsors (federal, state, or private), collaborators, or others with regulatory, financial, intellectual property or other interests or rights to the data produced in the study or the data to be used in the study.

ss.05-PR.12
The signatories will maintain a joint working group to confer at least annually for the purpose of reviewing and maintaining the procedures by which to share the information necessary for an effective response to a public health event and to conduct joint communication and coordination of information before and during a public health event. Such procedures are set out in the most recently approved "[Region] Health Initiative Infectious Disease Emergency Communications Guideline."

mm.09-PR.12
4. Scope of Epidemiologic Events

The purpose of this chapter is to characterize the scope or range of epidemiologic events for which both countries agree that exchange of epidemiologic information is appropriate. It is understood that the information to be shared by one country be such that it leads to or facilitates action in the second country which will be of direct benefit to the health of the population of one or both countries. This would include:

mm.09-PR.12
A. Cases of disease identified in one country for which there is evidence or reason to suspect an epidemiologic link to the other country, including diseases detected in animals, or that such a link may occur in the future due to expected cross-border travel;

mm.09-PR.12
B. Similarly, the identification of risk factors for disease in one country which may lead to disease in the other country.

mm.09-PR.12
Types of epidemiologic events which meet these criteria include the following:

- A probable or confirmed case of a severe or otherwise important vector-borne infection occurring in the border region of a border state (e.g., dengue or West Nile Virus encephalitis).
- A probable or confirmed case of a severe or otherwise important infectious disease with high potential for spread to the other country.
- Infections in animals in the border region with potential for spread of severe disease to humans.
- A probable or confirmed case of severe disease suspected of having been intentionally spread.
- Disease outbreaks which involve both countries at the time of discovery or which have a significant potential for spread to the other country.
- Outbreaks of disease associated with travel or migration to the other country.

- Outbreaks of disease or chemical contamination associated with food or other products originating in the other country.
- Environmental health emergencies affecting both countries.
- Binational cases of notifiable diseases.

mm.09-PR.12
5. Procedures for Notification of Binational Cases—Clear mechanisms of notification should be agreed to by public health officials of both countries, at the different levels of government, which specify:

Counterpart agency and corresponding office to notify.
Channels for communication which minimize delay in receiving the notification.
Information to be included regarding the binational case(s).

mm.09-PR.12
6. Follow-up Information on Binational Cases—The two countries should exchange follow-up information on binational cases so that the effectiveness of binational case notification and coordinated case investigations can be determined.

mm.09-PR.12
Mechanisms for the transport of specimens or needed supplies through U.S. and Mexico customs.

mm.09-PR.12
3. Collaborative Investigations of Binational Outbreaks—Upon binational concurrence to conduct a binational investigation or response effort, a binational oversight team of public health officials from the two countries should meet. Unless defined otherwise, the coordination of the investigation will be the responsibility of the lead public health authority where the outbreak is to be investigated. The oversight team will be responsible for or coordinate:

- choosing the members of the binational field investigation team, including a lead from each country;
- field work preparation, including arrangements for any necessary travel, personal protective gear, prophylaxis, and availability of supplies and equipment;
- planning and implementation of the investigation;
- content of health alerts and press releases; and
- determination of control measures based on information provided by field staff.

mm.09-PR.12
5. Binational Cooperation in Sharing Epidemiology Resources—National and state public health agencies are encouraged to share informational and other resources designed to strengthen the epidemiology and response capacity of binational counterparts. Joint participation in multinational agencies (e.g., PAHO) and NGOs (e.g., TEPHINET) provides additional opportunities to identify such needs and appropriate tools which have been developed.

mm.09-PR.12
4. Resource Sharing in Emergencies—In preparation for such potential events,

agreements should be established between the public health authorities of the two countries—including local, state and federal levels—regarding the sharing of health resources during public health emergencies, together with expedited clearance procedures for cross-border transfer of such resources by immigration and custom officials, when such a public health emergency is formally declared.

mm.09-PR.12
5. Adherence to Outbreak Guidelines—Cooperation in the investigation of such incidents is strongly encouraged and should follow the same guidelines as for naturally occurring outbreaks.

mm.09-PR.12
6. Quarantine of Foreign Citizens—In the event that a quarantine is considered necessary by the public health agency of a country that will include citizens of the other country, this decision will be communicated urgently to the counterpart public health agency of the other country. The public health agency enacting the quarantine needs to recognize the special needs of citizens of the other country who are caught outside their place of residence, while still ensuring the effectiveness of the quarantine measure.

mm.09-PR.12
2. Transport of Laboratory Samples through Customs—In cases where specimens of public health interest need to be carried across the border for testing in a laboratory of the other country, mechanisms need to be established to assure expedited passage through customs, since excessive delay may compromise the quality of the specimen and the ability to obtain an accurate diagnosis. This is likely to require an advance agreement among the involved agencies, including the customs authority, specifying a clearly defined protocol to be followed for the rapid, cross-border transport of a set of specimens.

mm.09-PR.12
3. Standards for Sample Transport—Specimens being sent for testing in the neighboring country need to follow national and international standards for the labeling, packaging and transport of such material. In laboratories which may participate in such collaborative testing, specific training on implementation of these standards should be provided to responsible personnel in these areas, together with written instructions.

mm.09-PR.12
4. Authorized Request for Laboratory Testing—Submission of samples for diagnostic testing by a laboratory of the neighboring country should be preceded by communication between authorized public health officials of the two countries, with approval of the receiving laboratory. Upon arrival of the specimen, confirmation should be sent to the agency submitting the specimens for testing. In situations where there is potential for the laboratory to be sent a large number of specimens, the receiving laboratory should establish a triaging policy which defines the priority of received samples for urgent testing, and inform referring agencies of this policy.

mm.09-PR.12
Communications between Public Health Agencies

1. Existing Information Sources—To facilitate the exchange of information recommended in this document, public health agencies should consult and subscribe to those information outlets provided by the other country (e.g., publications, press releases, Boletín Epidemiología, Health Alert Network, Epi-X).

mm.09-PR.12
2. Inter-Agency Communications—Direct communications between corresponding programs and staff of counterpart agencies is encouraged (e.g., to contact a known staff member in the measles unit to report a case of binational interest). However for cases when program staff are not known or cannot be reached, or for emergencies and other broader issues of common interest, counterpart agencies of the two countries should each have a telephone contact number and email address which is staffed at all times for such communications. In the case of binational events requiring continued collaboration, the communications offices of counterpart agencies should be in regular contact, exchanging relevant information and coordinating the release of information to the public.

mm.09-PR.12
Release of Information to the Public

3. Harmonization of Public Information—In cases of binational epidemiologic events, information released to the public by the two countries regarding the event, risk factors and preventive measures, should be consistent, based on the best available scientific evidence of the event itself, and the pathogens or substances involved. Ideally, the population of each country should receive such information from their public health authorities in the same time period, to avoid creation of unexpected demands on public health authorities from one-sided releases, and to reinforce their credibility to the public.

mm.09-PR.12
4. Sharing of Information for the Public—In the case of a binational public health emergency or outbreak affecting the population of both countries, copies of information made available to the public by the respective public health agency should be shared with the counterpart agency of the other country. In non-emergency circumstances, such information should be made available on request.

mm.09-PR.12
5. Travel Notices—Travel notices are posted by public health authorities to provide information to travelers, the public, healthcare providers and public health authorities regarding outbreaks of disease of public health significance. The character of the notification is based on four criteria relating to disease transmission, containment measures, quality of surveillance, and quality and accessibility of medical care. In the case of such travel notices or other communications to the public which could have negative impact on trade, the counterpart agency should be given prior notice of the action to be taken and the evidence supporting that decision for their review and, if appropriate, their response.

hh.06-PR.12
Each Network will be responsible for initiating, updating, monitoring, controlling, and removing or suspending access of its Authorized Users. Each Network shall receive from each Authorized User contractual assurances that it will initiate, update, monitor, control and, where necessary, remove or suspend access of its Registered Users.

hh.06-PR.12
a. If an Authorized User allows its patients the right to prohibit the access of all their data from a particular encounter(s) through an Exchange, and the patient has chosen this option, the Network shall either exclude relevant data or require the Registered User to exclude such data.

sp.08-PR.12
Clinic is responsible for entering immunization information into the [IIS]. It is strongly recommended that data be entered daily.

ss.08-PR.12
1. The [DHSS] shall provide information or services in accordance with Section II (A.)3 which establishes the service deliverables which this agency must perform, in accordance with the established time frames established for each item in Section II (A)3.

ss.08-PR.12
The Participants shall be required to maintain all records for a period of time designated by their respective Department Record Retention Schedules.

ss.08-PR.12
3. The following deliverables are those agreed upon by the Participants:

ss.08-PR.12
Through an extract process, identified shared patient records will be selected from each collaborative partner’s data base, and a batch file will be created for transmission to the respective collaborative partner that requires the immunization information. The received immunization data will then be updated into the collaborative partner’s immunization database.

4.6 Software/Hardware (SH)

SH.01 Description of Software/Hardware Provided

sp.09-SH.01
[Program] Policies

[Program] Data Sharing and Security Framework (DSSF)

[Program] security policies for authentication (identity management) and authorization

pp.05-SH.01
2. In addition to operating its own database and information system [Entity] is licensed to provide access to the [Name] Profile Immunization Registry and Tracking System, a database system designed to store and communicate immunization information pertaining to adults and children in [State] State (“[Name] Profile”). The information available through the [Name] Profile system is intended to include as broad a portion of the population age six and under of the State of [State] as possible. Because some of the patient data contained in the [Name] Profile database has been obtained from sources other than providers who have entered into Health Care Provider Information Sharing Agreements with [Entity].

pp.05-SH.01
2. In addition to operating its own database and information system [Entity] is licensed to provide access to the [Name] Profile Immunization Registry and Tracking System, a database system designed to store and communicate immunization information pertaining to adults and children in [State] State (“[Name] Profile”). The information available through the [Name] Profile system is intended to include as broad a portion of the population age six and under of the State of [State] as possible. Because some of the patient data contained in the [Name] Profile database has been obtained from sources other than providers who have entered into Individual Provider Information Sharing Agreements with [Entity]:

pp.05-SH.01
The following services are available to the Provider under this agreement. These services are included in the standard package of [Name] Profile Information Services available from [Entity] under its agreement with the Joint Executive Management Team (JEMT) of the [County] Department of Health and the [Health District] to resell use of the [Name] Profile system to Providers in the state of [State]. The [Name] Profile system is operated by JEMT for the benefit of children, their care providers, health plans, public health agencies and other entities that are concerned with assuring the effective immunization of children. JEMT is solely responsible for the operation of the [Name] Profile system. [Entity]'s sole responsibility is to assist JEMT in the marketing of the [Name] Profile services in the State of [State].

pp.05-SH.01
The [Name] Profile system and database contains data about children in [State] State including demographic information and data on their immunization treatment history. The Provider will have full access to the [Name] Profile System and its online services features during the hours of 7:00 AM to 8:00 PM, Monday through Saturday of each week.

pp.05-SH.01
Use of the [Name] Profile system is made available to the Provider in accord with the guidelines and end-user procedures established in the [Name] Profile User Manual which is a part of this agreement.

Online Patient Record Queries and Immunization Record Access and Updating:

pp.05-SH.01
The provider, using a standard personal computer and modem, or a direct network connection to the [Name] Profile system, and whose identity has been established with the [Name] Profile system in accord with the user authentication procedures for the [Name] PROFILE system, can query the [Name] Profile database to ascertain whether his/her patient has a record in the [Name] Profile database. The provider can update the demographic data for the patient and/or create a new demographic record.

pp.05-SH.01
The provider can also query the database to view the record of immunization treatment events for the patient, create a new record for a new immunization, and record notes regarding patient conditions that may be useful in subsequent immunization treatment decisions. Vaccine manufacturer lot numbers can be recorded for the treatment event. The system also records the user identity of the person updating the record.

pp.05-SH.01
The provider can also obtain recommendations for immunization treatments for the child based on the immunization schedule algorithm used by the [Name] Profile system for evaluating the immunization status of a child. This algorithm is based on the pediatric immunization schedule published by the U.S. Centers for Disease Control with the advice of the American Academy of Pediatrics.

pp.05-SH.01
Providers will receive at their computer workstation patient-specific and vaccine-specific listings to be used by their office to notify patients prior to a scheduled immunization, or to follow up with a patient when a scheduled immunization has not been completed on a timely basis. This information will be provided to the provider at the provider's option in two forms: a list of patients and their phone numbers which can be printed on a standard computer

printer, or images containing the mailing address of the child which can be printed on standard mailing label forms.

pp.05-SH.01
Reports to a provider of an individual patient's immunization history. Reports are printed either on the physicians local office printer or on their fax machine.

pp.05-SH.01
Customized reports for medical clinics and physician offices that describe the status of current vaccine inventory, the total number of doses of vaccine delivered during the previous month, and additional supplies needed by the clinic/office can be prepared as required and defined by the State Department of Health's Vaccine Distribution Program.

pp.05-SH.01
2. In addition to operating its own database and information system [Entity] is licensed to provide access to the [Name] Profile Immunization Registry and Tracking System, a database system designed to store and communicate immunization information pertaining to adults and children in [State] State ("[Name] Profile"). The information available through the [Name] Profile system is intended to include as broad a portion of the population age six and under of the State of [State] as possible. Because some of the patient data contained in the [Name] Profile database has been obtained from sources other than providers who have entered into Individual Provider Information Sharing Agreements with [Entity]:

pp.05-SH.01
The following services are available to the Provider under this agreement. These services are included in the standard package of [Name] Profile Information Services available from [Entity] under its agreement with the [Team] of the [County] Department of Health and the [Health District] to resell use of the [Name] Profile system to Providers in the state of [State]. The [Name] Profile system is operated by [Team] for the benefit of children, their care providers, health plans, public health agencies and other entities that are concerned with assuring the effective immunization of children. [Team] is solely responsible for the operation of the [Name] Profile system. [Entity]'s sole responsibility is to assist [Team] in the marketing of the [Name] Profile services in the State of [State].

pp.05-SH.01
The [Name] Profile system and database contains data about children in [State] State including demographic information and data on their immunization treatment history. The Provider will have full access to the [Name] Profile System and its on-line services features during the hours of 7:00 AM to 8:00 PM, Monday through Saturday of each week.

pp.05-SH.01
Use of the [Name] Profile system is made available to the Provider in accord with the guidelines and end-user procedures established in the [Name] Profile User Manual which is a part of this agreement.

pp.05-SH.01
The provider, using a standard personal computer and modem, or a direct network connection to the [Name] Profile system, and whose identity has been established with the [Name] Profile system in accord with the user authentication procedures for the [Name] PROFILE system, can query the [Name] Profile database to ascertain whether his/her patient has a record in the [Name] Profile database. The provider can update the demographic data for the patient and/or create a new demographic record.

pp.05-SH.01
The provider can also query the database to view the record of immunization treatment events for the patient, create a new record for a new immunization, and record notes regarding patient conditions that may be useful in subsequent immunization treatment decisions. Vaccine manufacturer lot numbers can be recorded for the treatment event. The system also records the user identity of the person updating the record.

pp.05-SH.01
The provider can also obtain recommendations for immunization treatments for the child based on the immunization schedule algorithm used by the [Name] Profile system for evaluating the immunization status of a child. This algorithm is based on the pediatric immunization schedule published by the U.S. Centers for Disease Control with the advice of the American Academy of Pediatrics.

Reminder/Recall:

pp.05-SH.01
Providers will receive at their computer workstation patient-specific and vaccine-specific listings to be used by their office to notify patients prior to a scheduled immunization, or to follow up with a patient when a scheduled immunization has not been completed on a timely basis. This information will be provided to the provider at the provider’s option in two forms: a list of patients and their phone numbers which can be printed on a standard computer printer, or images containing the mailing address of the child which can be printed on standard mailing label forms.

Individual Immunization History Reports:

pp.05-SH.01
Reports to a provider of an individual patient's immunization history. Reports are printed either on the physicians local office printer or on their fax machine.

Vaccine Distribution Reports:

pp.05-SH.01
Customized reports for medical clinics and physician offices that describe the status of current vaccine inventory, the total number of doses of vaccine delivered during the previous month, and additional supplies needed by the clinic/office can be prepared as required and defined by the State Department of Health’s Vaccine Distribution Program.

ph.06-SH.01
8. Software and/or Hardware Provided by [SNO Name]. The Model assumes that the SNO will provide some of the software and/or hardware Participants would use to access the System. If the SNO does not provide software and/or hardware to Participants, this section would be omitted. The specific language shown in this section is for illustration only. The SNO will need to tailor the language of this section to the limitations imposed by the SNO’s software and hardware vendor(s).

ph.06-SH.01
8.1 Description. A description of any software and/or hardware that the SNO will provide to Participants. [SNO Name] shall provide to each Participant the software and/or hardware required to access the System and use the Services the Participant has registered to receive, as more particularly described on Schedules 8.1(a) (Software) and 8.1(b) (Hardware) (the “Associated Software” and “Associated Hardware,” respectively).

ph.06-SH.01
The Model assumes that the SNO will provide some of the software and hardware that Participants will require to use the System, as described in Section 8 (Software and Hardware Provided by [SNO Name]), and that the Participant will be required to provide the remainder (e.g., a personal computer with an operating system and web browser meeting certain specifications), as described in Section 10.3 (Software and Hardware Provided by Participant). The terms of Section 8 (Software and/or Hardware Provided by [SNO Name]) and Section 10.3 (Software and Hardware Provided by Participant) should be revised as necessary to conform to each other. The Model assumes that Stark and Anti-Kickback law issues that, depending upon the relationship of the SNO to its Participant, may arise from the SNO's provision of software, hardware and services, will have been resolved.

sp.02-SH.01
6. Information to be Provided to Participant by [Program].

a. The Information Services Available to Participant under this Agreement are set forth in Appendix A. The [Program] Management Committee may make additional or enhanced information services available to the Participant from time to time, by written notice including identification of the additions or enhancements and any associated cost increase or reduction. Such amendments shall be incorporated into this Agreement and the contractual relationship between the parties, and become effective upon written communication of the amendment by the [Program] Management Committee to the Participant. Such amendments shall not effect the other provisions of this Agreement.

sp.02-SH.01
[Program] INFORMATION SERVICES AVAILABLE TO PARTICIPATING PROVIDERS

The [Name] Program provides a vehicle through which health care providers can reliably collect and analyze relevant outcomes data. The benefits of this approach are twofold: (1) the measurement process is provider-driven and (2) the results of the process represent a proven method to effectively satisfy specified internal and external performance measurement needs. Through its physician-led Management Committee and information service offerings, [Program] will accomplish the following objectives:

1. Collect and aggregate condition-specific clinical data using consensus generated methods and data standards, thereby enabling analysis to be based on relevant clinical data;
2. Seek to identify clinical processes that lead to improved outcomes;
3. Facilitate outcome comparisons across participating providers to support internal quality improvement purposes and accreditation requirements; and
4. With approval by the [Program] Management Committee and the permission of data suppliers, i.e., the requesting Participants and/or their associated Providers, make information available to other parties as appropriate.

[Program] service offerings are directed at satisfying specific health data management and reporting needs of participating individual and institutional providers. [Program] services emphasize credible data collection, storage and analytic methods; secure data access and proper authorization for information reporting. [Program] services produce value by providing technical infrastructure and data processing capability to reduce the clinical information management burden for high volume, high cost diagnoses and procedures.

[Program] services will focus on cardiac surgery, percutaneous transluminal coronary angioplasty (PTCA), stents and other cardiac procedures and expand to include other modalities of clinical care. Under [State] state's current law, [Program] services are certified as a quality improvement effort, thereby protecting provider data from public disclosure.

The following services will be provided by [Program]:

- Basic service package
  - Customer support
  - Secure and confidential data storage
  - Advanced statistical analyses, including risk adjustment
  - Standard institutional and comparative outcomes reporting
- Fee-for-service options
  - Custom institutional and physician outcomes reporting
  - Data collection assistance
  - Authorized data access
  - Performance improvement consultation
  - ORYX data submission to JCAHO

[Program] SERVICE DESCRIPTIONS

Use of the [Program] Cardiac Registry is made available to Participants and their associated Providers in accordance with the guidelines and end-user procedures established in the Health Care Provider Procedure Manual. The following services are available to the Participants and their associated Providers under this Agreement:

BASIC SERVICES

Customer Support

The [Program] Cardiac Registry and related services are intended to directly support specified data management and reporting activities of practicing physicians and their affiliated institutions. As customers and end-users of the [Program] Cardiac Registry, Participants and their associated Providers will receive timely response to service inquiries and problem reports.

[Program] customer support will address issues pertaining to procedures outlined in the Health Care Provider Procedure Manual including data definitions, data submission, information system security, authorization, service descriptions, processing requests for fee-for-service options, and other issues as indicated.

Secure and Confidential Data Storage

[Program] will provide data management services that assure the integrity and safekeeping of longitudinal data including protecting against unauthorized access. Data protections will be enforced at institutional, provider and patient levels as per the [Program] Health Care Provider Information Sharing Agreement, [Program] policy and prevailing law. [Program] must have specific authorization by the Participant to perform analytical or reporting services.

Authorization for performance of the services included in the basic service package is assumed when Participants enter into the [Program] Health Care Provider Information Sharing Agreement.

Advanced Statistical Analyses

[Program] will use advanced statistical and analytical methods to process participant data into meaningful information. Where indicated, clinical information will be risk adjusted using agreed upon methods. Such methods will be determined based on a consensus decision by the [Program] Management Committee.

Standard Institutional and Comparative Outcomes Reporting

[Program] will develop and produce reports for Participants and their associated Providers who have authorized access to the information. Standard and custom reporting options will be offered. In the basic service package, standard reports will include data stratified by diagnosis, by institution. Standard institutional report formats to satisfy external compliance requirements will be offered.

[Program] will offer a standard outcomes report format for cross-institutional comparison. Such standard reporting will include "blinded" comparisons.

FEE-FOR-SERVICE OPTIONS

Custom Institutional and Physician Outcomes Reporting

Customized reporting for institutions and individual physicians may also be performed, as authorized. As part of this service, authorized Participants and their associated Providers may instruct [Program] to provide such reports to third parties, e.g., to satisfy JCAHO or NCQA requirements.

Customized comparative reporting will also be offered for health systems, networks or health care alliances as directed. Proper written authorization will be obtained from all Participants and their associated Providers that are included in any comparative report.

Data Collection Assistance

A Core Data Set of clinical measures has been defined for collection by [Program] Participants and their associated Providers. Functional measures that enable longitudinal outcomes assessment will be added as funding becomes available. Standard data collection methods include a fax-based system described in detail in the Health Care Provider Procedure Manual. Custom electronic interfaces for batch transmission may be developed by participating Providers at their expense.

Beyond facilitation of an operational fax-based system for Participants and their associated Providers, [Program] will provide on-site data collection assistance, for a nominal fee, as requested by participants.

Additional data selection and collection methods will be collaboratively developed by clinicians and administrative stakeholders. This consensus-based process will reflect the input of Participants and their associated Providers, thereby enhancing the perceived and actual value of [Program] services beyond that of other proprietary and non-standard information management and outcome reporting methods.

Authorized Data Access

Participants and their associated Providers will be granted authorized access to electronic copies of the raw data they have submitted as provided for in the [Program] Health Care Provider Information Sharing Agreement. Due to the labor and technology involved in processing such requests, authorized access to raw data will be billed as a separate fee for-service option.

Performance Improvement Consultation

For a nominal fee, [Program] will provide performance improvement consulting services related to the interpretation and use of standard and custom reports on institutional and cross-institutional performance.

ORYX Data Submission to JCAHO

[Program] will assist Providers in the satisfaction of accreditation requirements by the Joint Commission on Accreditation of Healthcare Organizations. At the request of participating providers, [Program] will submit data for selected performance indicators to JCAHO on behalf of Participants and their associated Providers.

1. Definitions

hh.06-SH.01
"Documentation" means the user documentation, manuals, and user guides, whether in paper, electronic, or other form, furnished to a Network by the other for use with the Exchanges.

mm.10-SH.01
Expected Knowledge and References

It is assumed that the reader has a working knowledge of the IHE ITI XDS Profile and its dependent Profiles which can be downloaded from the IHE website: http://www.ihe.net/Technical_Framework/index.cfm

mm.10-SH.01
The key Integration Profiles and section number in the above document are:

XDS – Section 10
PIX – Section 5
PDQ – Section 8
ATNA – Section 9

mm.10-SH.01
In addition, the existing Cross Community Information Exchange and the Cookbook for the Security Sections of IHE Profiles White Papers, as well as Basic Patient Privacy Consents Supplement provide useful information regarding areas that should be addressed when implementing an XDS Affinity Domain. These can all be found using the IHE website link above.

mm.10-SH.01
XDS Affinity Domain Definition Template

The concept of an XDS Affinity Domain is defined in ITI TF-1:10 and Appendix K. It is clear that many regulatory/professional organizations will need to define policies regarding coded terminology, privacy, document format and content, language support, etc. for an XDS

Affinity Domain. This template provides a consistent documentation template for documenting implementation decisions, policies, and IHE Profile refinements, for either an individual XDS Affinity Domain, or multiple XDS Affinity Domains within a particular nation or region. In addition, its provides a comprehensive list of all relevant topics that should be considered for deployment of XDS Affinity Domains, and implementers may find it helpful in guiding their policy and refinement decisions.

mm.10-SH.01
System Architecture

In order to secure both information retrieval and publishing, the system architecture of the applications has to be specified and understood by all parties. The Policy Agreement shall therefore contain detailed information regarding the architecture of systems supporting the various Actor/Profiles, and the supported document types and publication policies.

mm.10-SH.01
Global Architecture

The XDS Affinity Domain global architecture diagram should be offered in this section indicating the stakeholders and system actors**.**

mm.10-SH.01
Access Control Policies

Privacy Consent Policy

Description

Billing Information

May be accessed by administrative staff and the patient or their legal representative.

Administrative Information

May be accessed by administrative or dietary staff or general, direct emergency care providers, the patient or their legal representative.

Dietary Restrictions

May be accessed by dietary staff, general, direct or emergency care providers, the patient or their legal representative.

Etc.

If access control policies are tied to specific user roles then an access control matrix should be specified here that links specific user roles to the types of documents that these users are permitted to access. The means for actually defining, and assigning these user roles should be specified in the _____ section

SH.02 Grant of Right/License to Receiver of Software/Hardware

ph.06-SH.02
8.2. Grant of License. A description of the Participant’s right to use the Associated Software and Hardware. [SNO Name] grants to each Participant a non-exclusive, personal, nontransferable, limited license to use the Associated Software and the Associated

Hardware for access to or use of the System and, if the Participant is a Data Recipient, for the purpose of obtaining the Services (the "Associated Software").

pp.06-SH.02
Section 6.03 Ownership of Network Equipment.

Through the First Agreement, certain Participants received computer hardware associated with the Network such as computers, printers, and communication lines. Such equipment obtained through the First Agreement and the contract between [State] University and the National Institutes of Health through the National Library of Medicine providing for the creation and maintenance of a [State] Regional Network for Primary and Emergency Care shall be and remain the sole property of NLM even though used by the Participants in their respective facilities.

From time to time, grants and contracts in which the Participants agree to participate that relate to the use and disclosure of the Information may provide for the purchase of additional equipment related to the Network. The ownership of any such equipment shall be governed by the relevant grant or contract.

Any equipment or communication lines supplied by individual Participants shall remain the sole property of the supplying Participant. Equipment, software, intellectual property, or communication lines supplied by [Organization] shall remain the sole property of [Organization], but shall be available for use by the Participants in conjunction with this Agreement.

hh.06-SH.02
3.2 Hardware and Software. Each Network shall acquire, install, provide, and properly maintain, at its own cost, the hardware and software including, without limitation, all of each Network's core systems necessary or appropriate to receive, access and utilize its Exchange, as permitted by this Agreement.

SH.03 Limitations on Copying and Other Requirements Related to Copying Software

ph.06-SH.03
8.3 Copying. Restrictions upon the Participant's right to copy software provided by the SNO.

Alternative One: Participant may not make copies. The Participant shall not, without [SNO Name]'s prior written consent, copy any of the Associated Software.

ph.06-SH.03
OR Alternative Two: Participant may make limited copies. The Participant may make one (1) copy of the whole or any part of the Associated Software in executable form for back-up or archival purposes; provided, that such copy must reproduce and include the copyright notice of [SNO Name].

SH.04 Restriction/Prohibition on Modification of Software

ph.06-SH.04
8.4 Modifications; Derivative Works. Restrictions upon the Participant's right to modify the System or the Services. The Participant shall not modify, reverse engineer, decompile, disassemble, re-engineer or otherwise create or permit or assist others to create the

Associated Software or the System otherwise, or to create any derivative works from the Associated Software or the System. The Participant shall not modify the Associated Software or combine the Associated Software with any other software or services not provided or approved by [SNO Name].

SH.05 Covenant to Execute All Licensing or Other Agreements Required by Third Party Vendors

ph.06-SH.05
8.5 Third-Party Software, Hardware, and/or Services. How the SNO and Participants will address requirements imposed by third-party software, hardware, and/or service vendors. The Associated Software includes certain third-party software, hardware, and services, which may be subject to separate licenses or subscription or other agreements or may require that a Participant enter into such agreements with third-party vendors. Each Participant shall execute such agreements as may be required for the use of such software, hardware or services, and to comply with the terms of any applicable license or other agreement relating to third-party products included in Associated Software.

SH.06 Miscellaneous Software/Hardware Provisions

pp.06-SH.06
Section 6.05 Use of Network Equipment. The Participants agree that any equipment associated with the Network, whether supplied by [Organization] or a Participant, shall not be used in any way that interferes with Network-based activity.

ph.06-SH.06
A sample online Registration Form is attached as Exhibit 1 (Registration Application and Agreement). Online registration offers a mechanism for collecting Participant information and effecting Registration Agreements efficiently, but it is recognized that the SNO should review and approve and/or authenticate each registration (see Section 4.3.3 (Approval and Disapproval of Registration Forms) and Section 4.3.4 (Acceptance of Registration)) and assure that Participants are appropriately trained in not only the use of the System and the Services but also in the Participant's legal obligation to comply with the terms of its Registration Agreement (see Section 10.5 (Training)).

ph.06-SH.06
A sample online Registration Form is attached as Exhibit 1 (Registration Application and Agreement). Online registration offers a mechanism for collecting Participant information and effecting Registration Agreements efficiently, but it is recognized that the SNO should review and approve and/or authenticate each registration (see Section 4.3.3 (Approval and Disapproval of Registration Forms) and Section 4.3.4 (Acceptance of Registration)) and assure that Participants are appropriately trained in not only the use of the System and the Services but also in the Participant's legal obligation to comply with the terms of its Registration Agreement (see Section 10.5 (Training)).

pp.06-SH.06
[Organization] will provide, at its own cost, the computer software necessary to allow Participants to store and access Information on the Network and will arrange for the installation of, and bear the cost of, the necessary communication lines and/or encryption devices (at [Organization]'s discretion) to allow the secure transfer of the Information to and from the Network by the Participants to the extent that the Participants do not already maintain such lines or devices. [Organization] will also provide personnel to assist with the mapping of test results and physician codes into a standard form accessible by all

Participants. [Organization] will also provide support for initial training, troubleshooting, and maintenance of equipment it provides that is used for Network connectivity. Except as provided Section 6.02(a), to the extent that Participants do not have equipment (including, but not limited to computers and printers) that was supplied in conjunction with the First Agreement for use in accessing the Network, the Participants shall use their own existing equipment to access the Network (e.g., video terminals, printers at Participants' sites) and all Participants shall provide other necessary supplies such as printer paper, ink cartridges, and toner, as is the current practice.

pp.06-SH.06
Section 6.06 Cooperation With [Organization].

The Participants agree to provide assistance and cooperate with [Organization] with regard to the installation and maintenance of the software or equipment necessary to store Information on and access the Network. The Participants agree to exercise reasonable care in the use of the equipment provided by [Organization] (and any equipment previously provided through the First Agreement), and further agree to immediately notify [Organization] or its designee upon the malfunction of any of said equipment.

The Participants agree to cooperate in the process of standardized coding of physician orders and test results.

sp.09-SH.06
The [Entity] security policies and procedures set forth the requirements for providing the software and procedural infrastructure that provides the levels of access controls for each dataset as determined by the data-providing institution.

ph.06-SH.06
11. [SNO Name]'s Operations and Responsibilities. Provisions describing the role and responsibilities of the SNO.

ph.06-SH.06
The Model assumes that the SNO will provide a variety of services to Participants. Responsibilities may include:

- System support
- Installation support
- Initial and ongoing training
- Help desk
- Problem resolution
- Auditing and reporting access and use
- Reporting unauthorized uses and security incidents

Some examples are provided for purposes of illustration.

ph.06-SH.06
11.2 Maintenance of System. The SNO's obligations to maintain the functionality of the System and the Services, and to provide updates. [SNO Name] shall maintain the functionality of the System and the Services in accordance with the Common Framework Policies and Procedures, and shall provide such service, security, and other updates as [SNO Name] determines are appropriate from time to time.

ph.06-SH.06
11.3 Training. The SNO's obligations to provide training for Participants and/or its Authorized Users. [SNO Name] shall provide training to each Participant [and/or Authorized User] regarding the Participant's [and/or the Authorized User's] rights and obligations under its Registration Agreement and the Terms and Conditions, and the access and use of the System and Services, including such user manuals and other resources [SNO Name] determines appropriate to support the System and Services, including without limitation training for new or additional Authorized Users when added by the Participant.

ph.06-SH.06
11.4 Telephone and/or E-Mail Support. The SNO's obligations to provide support for the Participant's use of the SNO's System and/or Services.

Alternative One: SNO provides help desk functions. [SNO Name] shall provide, by telephone and/or e-mail, during normal business hours, support and assistance in resolving difficulties in accessing and using the System and the Services.

ph.06-SH.06
OR Alternative Two: SNO supports the Participant's help desk. [SNO Name] shall provide, by telephone and/or e-mail, during normal business hours, support and assistance to the Participant's help desk or other facility that supports use of the System and Services by Authorized Users.

ph.06-SH.06
11.5 Audits and Reports. Audits the SNO is to perform and reports it is to provide to Participants. [SNO Name] shall perform the following audits and provide the following reports to each Participant:

ph.06-SH.06
11.5.1 Usage Reports. [Specified statistical reports regarding the Participant's usage of the Services].

ph.06-SH.06
11.5.2 Reports to Public Agencies. [Specified reports that certain Participants may be required to make to public health agencies.]

ph.06-SH.06
11.5.3 Audit Trail Reports. [Specified reports that pertain to audit trail tracking.]

mm.10-SH.06
Daily Governance

Describe how the components of the XDS Affinity Domain are managed at an operational level. Considerations to comment on include, but are not limited to:
Overall operation management (coordination of efforts)
Sub-component division (if any)
Day-to-day operations management communication methods (meetings, summits, forums, etc.)

mm.10-SH.06
Configuration Management

Specify how change management issues (such as hardware upgrades, software upgrades, configuration changes, etc) are to be managed. Explain what authorization is needed in order to make changes to a component of the XDS Affinity Domain that will affect other components (such as those that will cause component downtime, require configuration changes on other systems, or effect functionality).

mm.10-SH.06
Define how configuration settings will be disseminated among systems in the XDS Affinity Domain.

mm.10-SH.06
Addition of New Components

Specify procedures for adding new components to the XDS Affinity Domain. Explain who is authorized to grant permission for new components to be added and how are they can be contacted. Define procedures for providing the necessary configuration and security information to the managers of components that will need to communicate with a new component.

Define rules for moving of systems, particularly XDS Repositories.

mm.10-SH.06
Disaster Recovery

Define disaster recovery practices for the various types of components of the XDS Affinity Domain. Define procedures to follow when disaster recovery is needed, and what notification must be provided in such cases.

mm.10-SH.06
Future system developments

The Policy Agreement shall commit all parties to develop their future system according to this and other accepted standards in order to facilitate future co-operation for information transfer between their systems.

mm.10-SH.06
All these functions shall be specified in the Policy Agreement. The standardized layout of the Policy Agreement is described in Annex B of this document and shall be used as a guide when Policy Agreements are established.

mm.09-SH.06
Emergency Communications Channel—The program units for public health emergencies in the two countries, including their directors, should be known to each other. Both program units should have a mechanism permitting direct contact on a continuous basis (i.e., 24 hours/day, 7 days/week, 365 days/year).

4.7 Privacy (PY)

PY.01 Compliance with HIPAA Privacy Generally

pp.06-PY.01
Section 8.11 Notice of Privacy Practices. Each Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance

with 45 CFR § 164.520, as well as any changes to such notice. Each Covered Entity shall ensure that its Notice of Privacy Practices includes provisions that adequately inform Individuals: (a) that their PHI may be used and disclosed and received from other health care providers for Treatment purposes; (b) of the research uses and disclosures of PHI set forth in this Agreement; and (c) that their PHI may be used and disclosed by Business Associate to perform functions like those allowed in this Agreement.

pp.06-PY.01
Section 8.12 Limited Data Set Provisions. With regard to Limited Data Sets used by [Organization], the following provisions of this Article shall apply to the use and disclosure of such Limited Data

pp.06-PY.01
Section 8.13 Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure in violation of the requirements of this Agreement.

sp.07-PY.01
All records are considered confidential and covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

sp.07-PY.01
All records are considered confidential and covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Processes and Best Practices

SP.09-PY.01
Suggestions for conducting the informed consent process in a manner that permits data to be shared via the [Network] and utilizes, when appropriate, model informed consent language (see below)

ph.02-PY.01
a. Policies and procedures to prevent any use or disclosure of data subject to this Agreement, contrary to the requirements of this Agreement.

b. Joint Obligations to Maintain Enrollee Privacy:

ph.06-PY.01
Although [State Organization] is not a Covered Entity, this Agreement is entered into for the purpose of protecting the confidentiality and security of patient information transmitted or communicated to the above Patient as part of or in connection to the Network and for complying with the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, 45 C.F.R. Parts 160 and 164 ("HIPAA").

ph.06-PY.01
Compliance with Law. [State Organization] shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which [State Organization] reasonably believes: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party

to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally-funded healthcare program, including the Medicare and Medicaid programs.

EXHIBIT A

ph.06-PY.01
[State Organization] Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

[State Organization] is not a Covered Entity, as defined by the Health Insurance Portability and Accountability Act (HIPAA). This Notice of Privacy Practices is provided to you as a courtesy and in relation to various business associate relationships that [State Organization] may enter. This notice describes how we may use or disclose your PHI, with whom PHI may be shared, and the safeguards we have in place to protect PHI. This notice also describes your ability to access or amend your PHI. We are required to abide by the terms of the notice currently in effect, however, we reserve the right to change the terms of this notice and make the new notice provisions effective for all PHI that it maintains. If this notice is revised or updated, you will promptly receive a revised notice.

ACKNOWLEDGMENT OF RECEIPT OF THIS NOTICE

You will be asked to provide a signed acknowledgment of receipt of this notice. Our intent is to make you aware of the possible uses and disclosures of your PHI. The delivery of your healthcare services will in no way be conditioned upon your signed acknowledgment. If you decline to provide a signed acknowledgment, we will continue to provide your services, and will use and disclose your PHI for treatment, payment and operations when necessary.

HOW WE PROTECT YOUR PHI

We protect your PHI a variety of ways. For example, we authorize individuals to access your PHI only to the extent necessary to conduct treatment, payment or health care operations, such as exchange of prescription information between providers. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to disciplinary action if they violate them. When we share information with third parties, they are also required to maintain the confidentiality of your PHI. Our privacy policy and practices apply equally to current and former members, so you can be assured that we will maintain your confidentiality even if you no longer retain services from us.

INFORMATION WE OBTAIN

We obtain PHI that we need to conduct our normal business functions and to comply with the law. Examples of your PHI include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, billing information, etc.

We obtain most of your PHI directly from you or your exchanges with other parties. We may also obtain information from third parties related to your finances, employment, medical history, and other PHI. These third parties may include agents, employers, health care providers, other health plans or insurers, and state and federal agencies.

ph.06-PY.01

WHEREAS, Although [State Organization] is not a Covered Entity under HIPAA, this Agreement is entered into for the purpose of protecting the confidentiality and security of patient information transmitted or communicated to Provider as part of or in connection to the Network and for complying with Provider's obligations under the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, 45 C.F.R. Parts 160 and 164 ("HIPAA").

ph.06-PY.01

WHEREAS, Although [State Organization] is not a Covered Entity under HIPAA, this Agreement is entered into for the purpose of protecting the confidentiality and security of patient information transmitted or communicated to Provider as part of or in connection to the Network and for complying with Provider's obligations under the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations on privacy and security, 45 C.F.R. Parts 160 and 164 ("HIPAA").

ph.06-PY.01

B. [State Organization] agrees to not use or further disclose PHI other than as authorized by this Agreement or as required by law.

mm.06-PY.01

Provider personnel must take reasonable steps to protect the privacy of all verbal exchanges or discussions involving PHI (regardless of where the discussion occurs) by following appropriate Provider policies and procedures.

It is understood that in certain work environments Uses or Disclosures that are incidental to an otherwise permitted Use or Disclosure may occur, and such incidental Uses or Disclosures are not considered a violation provided that Provider has met the reasonable safeguards and minimum necessary requirements (if applicable).

ph.06-PY.01

5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-PY.01

9. Protected Health Information. Provisions addressing compliance with applicable laws addressing the confidentiality, security, and use of patient health information.

ph.06-PY.01

9.1 Compliance with Policies and Procedures. Provisions requiring compliance with the Common Framework Policies and Procedures. [SNO Name] and each Participant shall comply with the standards for the confidentiality, security, and use of patient health information, including without limitation protected health information described in HIPAA, as provided in the Common Framework Policies and Procedures, which is incorporated herein by reference. Each Participant shall comply with such standards regardless of whether or not that Participant is a "covered entity" under HIPAA.

mm.09-PY.01
Is your institution a covered entity as defined by the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (i.e., has your institution determined that it is subject to the requirements of the HIPAA Privacy Rule)? Describe the purpose and objectives of the project, the tools that will be adopted, and how the tools are expected to help achieve the purpose and objectives.

mm.09-PY.01
If the institution (or relevant component) is covered by the HIPAA Privacy Rule, state whether the health information to be shared includes direct identifiers, or only limited or de-identified data sets, as defined by the Rule (see chart below for guidance). If the dataset is de-identified, describe the process, whether manual or automated, used to deidentify it.

sp.02-PY.01
D. The parties acknowledge that the data provided for purposes of [Program] includes information about patients which the Participant is required to protect under federal and state laws.

sp.02-PY.01
(x) Protected Information means any information which identifies or could reasonably be believed could identify a Data Subject, which in any way concerns that Data Subject's health status, healthcare, or payments for his or her health care, or which a party is otherwise legally required to protect under an Information Protection Law applicable to that party.

mm.09-PY.01
The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule regulates how "covered entities"—e.g., healthcare providers, health plans, health billing services—use and disclose certain individually identifiable health information. While CDC is not considered a "covered entity," some state and local health departments may be. The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to "protected health information" (PHI) to carry out their public health mission. The Privacy Rule permits covered entities to disclose PHI, without authorization from the subject, to public health authorities (e.g., CDC, State and local health departments) that are legally authorized to receive such reports for purposes of preventing or controlling disease, injury, or disability. This includes, for example, reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. At the direction of a public health authority, covered entities may disclose PHI to a foreign government agency that is acting in collaboration with a public health authority [45 CFR 164.512(b)(1)(i)].

hh.06-PY.01
Each Network shall assure that each Authorized User will include a clause in its Notice of Privacy Practices indicating that patient data may be provided to third parties in various formats. The clause shall be substantially as follows:

"In order to efficiently coordinate the treatment, payment, and health care operations aspects of your care, we may disclose your PHI in any format that we determine is secure and expeditious, e.g., verbally, electronically, via fax, and/or in paper form."

6.3 Restrictions on Patient Information.

hh.06-PY.01
6. HIPAA.

6.1 Each Network represents and warrants that: (i) its Authorized Users shall access and use the Exchanges solely in their capacity as "covered entities," as that term is defined in 45 C.F.R. § 160.103; and (ii) each such access and use by an Authorized User shall be made solely for purposes of treatment, payment, and those health care operations specified in 45 C.F.R. § 164.506(c), or pursuant to a valid patient authorization or court order when required under 45 C.F.R. § 164.508, 45 C.F.R. § 2.1, et seq., and/or state law.

sp.08-PY.01
The [Immunization] Registry Security and Confidentiality Agreement must be signed by a representative of the participating health care entity or school, prior to any training on use of the [Immunization] Registry and gaining access to the Registry data. One or more persons from each site must complete the training for the [Immunization] Registry Site Administrator(s). Having completed the training, the Site Administrator(s) may enroll users who have been trained in the use of the [Immunization] Registry at the appropriate access level and have signed the [Immunization] Registry User Security and Confidentiality Agreement. The [Immunization] Registry Coordinator will maintain a file of signed [Immunization] Registry User Security and Confidentiality Agreements and will require new agreements to be signed by users every two years. The participating health care entity or school assumes responsibility for the individual's usage of the [Immunization] Registry. Providing access to [Immunization] Registry to outside organizations is strictly forbidden.

sp.08-PY.01
Participating immunization providers are expected to inform the child's parent, guardian or legal custodian that data may be transferred to the [Immunization] Registry and give the parent, guardian or legal custodian the opportunity to refuse to participate in the [Immunization] Registry. The [Immunization] Registry Disclosure Form, given at the time of immunization, can be used to provide this notice This form may be accessed directly from the [Immunization] Registry website.

ph.06-PY.01;
Hospital shall provide its employees who are granted Data User Accounts with education and training on HIPAA requirements to maintain the confidentiality of patient information accessed through Exchange.

mm.06-PY.01
Authorized Users shall use the Exchange solely to access patient information in the following situations:

mm.06-PY.01
Each Network member hospital will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

If a Network member hospital, following an investigation of an alleged violation, concludes that one of its Authorized Users has inappropriately accessed information of a patient treated at that hospital, the hospital will follow its internal policies and procedures to sanction the user.

If a Network member hospital, following an investigation of an alleged violation, concludes that a user authorized by another hospital has inappropriately accessed information of a patient treated at the first hospital, the first hospital will contact the authorizing hospital and request that the authorizing hospital follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing hospital thereafter shall notify the first hospital in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first hospital concludes that the same user has inappropriately accessed patient information a second time, that hospital will request that the authorizing hospital revoke the user's privileges to use Exchange. Any disputes between hospitals about sanctions of users will be resolved by the Exchange Task Force, whose conclusion shall be final.

If a Exchange member hospital determines that a breach has occurred, the hospital will notify Network. Network will then notify other hospitals of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their data.

Availability of Patient Information

Hospital Privacy Notices. Each Network member hospital will include a clause in its Notice of Privacy Practices indicating that patient data may be provided to third parties in various formats. The clause shall be substantially as follows:

"In order to efficiently coordinate the treatment, payment, and health care operations aspects of your care, we may disclose your PHI in any format that we determine is secure and expeditious, e.g., verbally, electronically, via fax, and/or in paper form."

"Para coordinar eficientemente el tratamiento, el pago, y los aspectos de la operación del cuidado de la salud, es posible que publiquemos su PHI en cualquier formato que determinamos es seguro y conveniente, por ejemplo, verbalmente, electronicamente, por medio de fax, y/o en palabra escrita."

sp.08-PY.01
Any Intermediary to which Protected Information is Disclosed must enter into a Written agreement requiring the Intermediary to Protect such Information which is consistent with and provides at least as much Protection for Protected Information as this Agreement;

The Intermediary has been identified in the applicable Specifications Addendum; and

The use of an Intermediary shall not relieve any party of any obligation stated in this Agreement, unless the parties expressly agree otherwise in Writing.

Information Protection Obligations of Disclosing Parties.

General Obligations. When Disclosing information under this Agreement, the Disclosing Party shall:

Maintain the policies, procedures and documentation necessary to establish the Disclosing Party's right and authority to Disclose that information.

sp.08-PY.01
Provide the Minimum Necessary Information as shown or stored in records or systems owned or operated by or subject to the Disclosing Party's control.

PY.02 Compliance with State Law

pp.05-PY.02
[Entity] intends to ensure that its privacy and security policies and practices meet or exceed the standards set by state and federal law for the privacy protection of individual health information. The parties therefore agree that:

pp.05-PY.02
1. [Entity] may amend these Obligations (a) in order to comply with newly enacted or amended state or federal laws or regulations, (b) in response to a previously unanticipated risk of breach of privacy which may become apparent in the operation of the information system, (c) in order to adopt standards, features or procedures which [Entity] may deem more effective in the protection of privacy, or (d) in order to adopt other new or enhanced information system standards, feature or procedures, so long as such new standards, features or procedures do not reduce or interfere with established privacy protections. Such amendments will be incorporated into this agreement in the form of amendments to [Entity]'s Insurance User's Manual, and will become effective upon [Entity]'s communication of the change to the Provider in writing. Such amendments shall not affect the other provisions of this contract.

pp.05-PY.02
[Entity] intends to ensure that its privacy and security policies and practices meet or exceed the standards set by state and federal law for the privacy protection of individual health information. The parties therefore agree that:

pp.05-PY.02
1. [Entity] may amend these Obligations (a) in order to comply with newly enacted or amended state or federal laws or regulations, (b) in response to a previously unanticipated risk of breach of privacy which may become apparent in the operation of the information system, (c) in order to adopt standards, features or procedures which [Entity] may deem more effective in the protection of privacy, or (d) in order to adopt other new or enhanced information system standards, feature or procedures, so long as such new standards, features or procedures do not reduce or interfere with established privacy protections. Such amendments will be incorporated into this agreement in the form of amendments to [Entity]'s User's Manual, and will become effective upon [Entity]'s communication of the change to the Provider in writing. Such amendments shall not affect the other provisions of this contract.

pp.05-PY.02
[Entity] intends to ensure that its privacy and security policies and practices meet or exceed the standards set by state and federal law for the privacy protection of individual health information. The parties therefore agree that:

pp.05-PY.02
i) [Entity] may amend these Obligations (a) in order to comply with newly enacted or amended state or federal laws or regulations, (b) in response to a previously unanticipated risk of breach of privacy which may become apparent in the operation of the information system, or (c) in order to adopt standards and procedures which [Entity] may deem more effective in the protection of privacy. Such amendments will be incorporated into this agreement in the form of amendments to [Entity]'s User's Manual, and will become effective upon [Entity]'s communication of the change to the Provider in writing. Such amendments shall not affect the other provisions of this contract.

ph.06-PY.02
Access to Specific Information and Providers. [State Organization] recognizes that certain categories of information, including but not limited to HIV status, mental health records and substance abuse records, may be more sensitive and may be accorded extra protections under state and federal law. Accordingly, as technology permits, [State Organization] will allow Patient to limit access to specific categories of information or specific providers as they see fit.

ph.06-PY.02
Compliance with Law. [State Organization] shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which [State Organization] reasonably believes: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally-funded healthcare program, including the Medicare and Medicaid programs.

ph.06-PY.02
B. [State Organization] agrees to not use or further disclose PHI other than as authorized by this Agreement or as required by law.

ph.06-PY.02
9.2 Additional Requirements. Provisions requiring compliance with patient information privacy, security, and use laws imposed at the state and/or local level. [SNO Name] and each Participant shall comply with the requirements for the privacy, security, and use of patient health information imposed under the laws of the State of _______________. Without limiting the generality of the foregoing, [SNO Name] and each Participant shall comply with the following: [list of state or local legal requirements, if desired].

mm.09-PY.02
If the institution is subject to regulations governing health data privacy or restricting access to certain data such as genetic data, describe any restrictions.

sp.02-PY.02
D. The parties acknowledge that the data provided for purposes of [Program] includes information about patients which the Participant is required to protect under federal and state laws.

sp.02-PY.02
a. The [Program] Program facilitated by [Entity] is an approved Coordinated Quality Improvement Program (“CQIP”) subject to the protections against disclosure provided in RCW 43.70.510 in the State of [State], and to equivalent protections in other jurisdictions where applicable

mm.09-PY.02
4. Confidentiality and Information Sharing—Public health agencies and food safety regulatory agencies are legally obliged in both countries to maintain the confidentiality of patient identification and trade secret information. However, quickly sharing specific information among relevant agencies in both countries on the number and locations of persons who have become ill, the associated epidemiologic information implicating food vehicles, as well as the point of origin and total distribution of the implicated foods, is

important to the rapid, appropriate and effective response to a binational outbreak of foodborne disease. The parameters that define which data must be shared and the conditions under which data sharing can legally occur should be determined in advance of binational food safety emergencies.

mm.09-PY.02
Protecting the privacy of patients and the security of information contained in the [Immunization] Registry is a high priority for the [City] Department of Public Health.

PY.03 Breach of Confidentiality (Improper Use of Data)

ph.02-PY.03
8. Reporting of Unauthorized Uses or Disclosures. In the event RESEARCHER becomes aware of any use or disclosure of data subject to this Agreement for any purpose or by any person or individual not authorized under this Agreement, RESEARCHER shall promptly notify the Data Provider. RESEARCHER shall require all contractors, employees and agents authorized to act on its behalf to notify RESEARCHER of any such use or disclosure they become aware of.

ph.06-PY.03
Mitigation of a breach of confidentiality (as defined in the [State Organization] Breach of Confidentiality Policy) or unauthorized access of PHI.

Payment for healthcare services.

Auditing and monitoring compliance with the terms and conditions of this Agreement.

ph.06-PY.03
Mitigation of a breach of confidentiality (as defined in the [State Organization] Breach of Confidentiality Policy) or unauthorized access of PHI.

Auditing and monitoring compliance with the terms and conditions of this Agreement.

ph.06-PY.03
L. [State Organization] agrees to regularly monitor and audit the access of each Network participant, and to take reasonable steps to pursue any breach or other privacy and security issues raised by such monitoring and auditing.

mm.06-PY.03
B. Process for Responding to Possible Violations.

Persons affiliated with the Provider, regardless of whether they have access to [State Organization], are encouraged to report possible breaches of confidentiality to the Provider’s Privacy Officer.

The Provider shall respond to possible violations in accordance with the Provider’s Security Policies and Procedures and general procedures for violation of Provider policy. The name of any persons involved with the possible violation shall be reported to [State Organization] within ten (10) days of the discovery of the violation.

A record of the event and any discipline imposed shall be maintained in the employee’s personnel file with a copy to be filed in a master file maintained by the Privacy Officer, and to be provided to [State Organization] within sixty (60) days of the event.

Appropriate Provider personnel are responsible for determining the severity of sanctions necessary, in accordance with Provider policies and procedures. A record of the final determination shall be maintained by Provider, to be provided to [State Organization] within sixty (60) days of the determination.

ph.06-PY.03

9.3 Reporting of Serious Breaches. Provisions requiring the SNO and Participant to report to each other concerning serious breaches of confidentiality of patient health information. Without limiting Section 9.4.7(Reports), if applicable to [SNO Name], [SNO Name] and Participant shall report to the other any serious use or disclosure of Protected Health Information not provided for by the Terms and Conditions of which [SNO Name] or Participant becomes aware, and any security incident concerning electronic Protected Health Information (a "Serious Breach of Confidentiality or Security"). A "Serious Breach of Confidentiality or Security" is one that adversely affects (a) the viability of the NHIN; (b) the trust among Participants or (c) the SNO's legal liability.

ph.06-PY.03

9.4.1 Use and Disclosure. [SNO Name] shall use and disclose Protected Health Information only for the purposes of [SNO Name]'s performance of its responsibilities described in the Terms and Conditions. Without limiting the foregoing, [SNO Name] may use and disclose Protected Health Information for the proper management and administration of [SNO Name]'s business and to carry out its own legal responsibilities; provided, that any disclosure pursuant to this Section 9.4.1 (Use and Disclosure) shall either be required by law or be made with reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to such person, and that the person will notify [SNO Name] of any instances of which it is aware in which the confidentiality of the information has been breached.

ph.06-PY.03

9.4.3. Reports to Participant. [SNO Name] shall report to the Participant any use or disclosure of Protected Health Information of the Participant not provided for by the Terms and Conditions of which [SNO Name] becomes aware, and any security incident concerning electronic Protected Health Information.

ph.06-PY.03

15.2.2 Specific Indemnities.

Provisions calling for special indemnification terms.

Alternative One: SNO and Participant indemnify each other for Serious Breaches of Confidentiality or Security for which they are responsible.

Notwithstanding Section 15.2.1 (Generally), [SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of any Serious Breach of Confidentiality or Security arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees.

sp.06-PY.03
16. The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made disclosure of the aforesaid file(s) that is not authorized by this Agreement or other written authorization from the appropriate System Manager or the person designated in item number 22 of this Agreement, CMS in its sole discretion may require the User to: (a) promptly investigate and report to CMS the User®s determinations regarding any alleged or actual unauthorized disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by CMS, submit a formal response to an allegation of unauthorized disclosure; (d) if requested by CMS, submit a corrective action plan with steps designed to prevent any future unauthorized disclosures; and (e) if requested by CMS, return data files to CMS. The User understands that as a result of CMS's determination or reasonable belief that unauthorized disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

sp.06-PY.03
17. The User hereby acknowledges that criminal penalties under 8 1106(a) of the Social Security Act (42 U.S.C. 8 1306(a)), including a fine not exceeding $5,000 or imprisonment not exceeding 5 years, or both, may apply with to disclosures of information that are covered by 8 1106 and that are not authorized by regulation or by Federal law. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. 8 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. 8 641 if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $1,000, they shall be fined under Title 18 or imprisoned not more than one year, or both.

ph.05-PY.03
To report to The Regents, through the Health System Privacy Officer, any use or disclosure of the Limited Data Set or any part of it not provided for by this Agreement of which User or any Authorized Party becomes aware.

PY.04 Business Associate

pp.06-PY.04
Section 8.01 Limits on Use and Disclosure.

Business Associate agrees to not use or further disclose PHI other than as permitted or required by this Agreement or as Required By Law. Business Associate may use and disclose PHI to perform those functions, activities, or services that Business Associate performs for, or on behalf of, each Covered Entity as specified in this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by a Covered Entity, including but not limited to storing Participant Information on the Network and maintaining the Network, making disclosures to Participants for Treatment purposes, using and disclosing Information for research purposes in compliance with ARTICLE VII, and reporting Information to appropriate governmental agencies for public health purposes (including, including, but not limited to, screening laboratory data on behalf of Covered Entities and making legally required reports to the [State] State Department of Health). Any such use or disclosure shall be limited to those reasons and those individuals as necessary to meet the Business Associate's obligations under this Agreement.

pp.06-PY.04
Business Associate will not make the following disclosures that are otherwise allowed to be made by a Covered Entity under 45 C.F.R. § 164.512 unless compelled to do so by law or unless such a disclosure is specifically authorized or required by this Agreement (including, but not limited to, ARTICLE VII):

About victims of abuse, neglect, or domestic violence:

- For health oversight activities;
- For judicial and administrative proceedings;
- For law enforcement purposes.

About decedents:

- For cadaveric organ, eye, or tissue donation purposes;
- To avert a serious threat to health or safety;
- For specialized government functions;
- For workers' compensation purposes;
- For marketing purposes;
- For fundraising purposes.

pp.06-PY.04
If Business Associate is requested to make a disclosure for one of the foregoing reasons, it shall forward such request to the Covered Entity so that the Covered Entity can coordinate and prepare a timely response. Business Associate shall make PHI available to the Covered Entity for the foregoing reasons if requested to do so in writing by the Covered Entity for the Covered Entity to coordinate and prepare a timely response.

Notwithstanding Section 8.01(a), Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Furthermore, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

pp.06-PY.04
If a Business Associate provides data aggregation services, the Business Associate may use PHI to provide data aggregation services to a Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B), except as otherwise provided by this Agreement.

ph.06-PY.04
III. Responsibilities of [State Organization] as a Business Associate:

[State Organization] and Provider acknowledge that under the Privacy Rule, Provider is a Covered Entity and [State Organization] is a Business Associate of the Provider with respect to certain [State Organization] duties. [State Organization] and Provider will be using and disclosing PHI. Accordingly, [State Organization] and Provider agree as follows:

[State Organization] may not use or disclose PHI in any manner that would constitute a violation of this Agreement or 45 C.F.R. Parts 160 and 164 if used or disclosed by Provider except that:

ph.06-PY.04
Notwithstanding any other provision of this Section 4 (Registration Agreements) to the contrary, if Section 9.4 (Business Associate Agreement) applies to a Participant's Registration Agreement, the Participant may terminate its Registration Agreement as set forth in Section 9.4.10 (Special Termination).

ph.06-PY.04
9.4 Business Associate Agreement. Provisions addressing the SNO's potential role as a business associate of the Participant. If, through any Data Recipient's use of the Services, [SNO Name]'s performance of its responsibilities described in the Terms and Conditions causes [SNO Name] to act as the "business associate" of the Data Recipient (as defined in 45 CFR Part 160.103), the provisions of this Section 9.4 (Business Associate Agreement) shall apply, in order to implement the requirements imposed under HIPAA for agreements between covered entities and their business associates. All capitalized terms not defined herein shall have the meanings given to them pursuant to 45 CFR Part 160.103.

sp.02-PY.04
b. The parties acknowledge that the Participant is a Covered Entity as defined in 45 CFR § 164.103, and that the Participant's privacy and information protection practices may be subject to requirements of both HIPAA and other Information Protection Laws. [Entity] is therefore the Participant's Business Associate as defined in 45 CFR § 160.103, and this Agreement is therefore intended to be interpreted consistently with the requirements for a Business Associate Contract under 45 CFR §§ 164.502(e) and 164.504(e).

hh.06-PY.04
12. Business Associate Addendum. Attached hereto is a copy of the Business Associate Agreement executed by the parties hereto [needed if purposes beyond TPO.]

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

PY.05 Use of Protected Health Information

sp.02-PY.05
(ii) Aggregation means the combination of Protected Information included in Participant Information with Protected Information received from another [Program] participant.

sp.02-PY.05
(iv) Health Care Operations means the various functions and activities identified under this definition at 45 CFR § 164.501.

A. [Entity]'s Obligation to Maintain Insurer Confidentiality:

pp.05-PY.05
[Entity] may from time to time receive requests from insurance companies, health plans, public health agencies, academic researchers or other interested parties seeking information which may pertain to insurers. [Entity] WILL NOT RELEASE ANY INFORMATION IDENTIFYING ANY INSURER, OR IDENTIFYING ANY HEALTH CARE SERVICES PROVIDED BY ANY PROVIDER PURSUANT TO ITS CONTRACT WITH ANY INSURER WHICH HAS SIGNED

THIS CONTRACT TO ANY SUCH PARTY WITHOUT THE WRITTEN CONSENT OF THE INSURER, EXCEPT IN THE EVENT THAT SUCH DISCLOSURE IS REQUIRED BY COURT OR AGENCY ORDER. IN THE EVENT OF SUCH AN ORDER [Entity] WILL CONTEST THE DISCLOSURE AND, UNLESS PROHIBITED BY LAW, SHALL GIVE THE INSURER PROMPT NOTICE OF ITS SERVICE.

ph.06-PY.05
1. Patient Access. [State Organization] hereby authorizes Patient to have access only to their own information contained in the Network and the Databases, for the following uses and purposes:

ph.06-PY.05
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network) to have access to his or her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.
- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-PY.05
We may use or disclose the PHI we obtain about you as described above with other third parties for treatment (e.g. assessing your needs), payment (e.g., evaluating claims) and/or healthcare operations (e.g., processing applications for services). Examples of other types of uses and disclosures include limited HIPAA compliant marketing, processing payments, administering contracts and processing transactions that you request. We may also disclose your PHI as permitted or required by law.

ph.06-PY.05
[State Organization] hereby authorizes Provider to have access to the Network and the Databases accessible through the Network for the following uses and purposes:

A. Treatment of a patient of or by Provider.

ph.06-PY.05
1. [State Organization] may use and disclose PHI if necessary for proper management and administration of [State Organization] or to carry out the legal responsibilities of [State Organization].

ph.06-PY.05
B. [State Organization] agrees to not use or further disclose PHI other than as authorized by this Agreement or as required by law.

ph.06-PY.05
9.4.1 Use and Disclosure. [SNO Name] shall use and disclose Protected Health Information only for the purposes of [SNO Name]'s performance of its responsibilities described in the

Terms and Conditions. Without limiting the foregoing, [SNO Name] may use and disclose Protected Health Information for the proper management and administration of [SNO Name]'s business and to carry out its own legal responsibilities; provided, that any disclosure pursuant to this Section 9.4.1 (Use and Disclosure) shall either be required by law or be made with reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to such person, and that the person will notify [SNO Name] of any instances of which it is aware in which the confidentiality of the information has been breached.

sp.06-PY.05
The User agrees that no findings, listing, or information derived from the file(s) specified in section 7, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a beneficiary's identification without first obtaining written authorization from the appropriate System Manager or the person designated in item number 22 of this Agreement. Examples of such data elements include but are not limited to geographic indicator, age, sex, diagnosis, procedure, admission/discharge date(s), or date of death. The User agrees further that CMS shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from CMS's files identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual to a reasonable degree of certainty.

sp.06-PY.05
The User agrees that, absent express written authorization from the appropriate System Manager or the person designated in item number 22 of this Agreement to do so, the User shall make no attempt to link records included in the file(s) specified in section 7 to any other identifiable source of information. This includes attempts to link to other CMS data file(s). The inclusion of linkage of specific files in a study protocol approved in accordance with section 6 is considered express written authorization from CMS.

ss.05-PY.05
Signatories will furthermore endeavor to protect data received from another signatory to the fullest extent permissible under law.

sp.02-PY.05
The Participant hereby authorizes [Entity] and its Subcontractors, under the oversight of the [Program] Management Committee, to use and disclose Participant Information as follows:

a. This authorization includes all information provided by or on behalf of the Participant, or derived from such information, including but not limited to information aggregated with information provided by other [Program] participants.
b. Provided that only the Minimum Necessary Participant Information (as defined below) is used or disclosed, [Entity] and its Subcontractors are hereby authorized:

(i) To review, analyze and process Participant Information to support [Program] participants in planning, quality assessment and improvement, and related functions;
(ii) To prepare Limited Data Sets (as defined in Section 4 and subject to the conditions of Section 3 below) derived from Participant Information, and to review, analyze and process such Limited Data Sets to support [Program] Participants in planning, quality assessment and improvement, and related functions, and for purposes of research;
(iii) To disclose any Participant Information to the Participant for purposes of the Participant's planning, quality assessment and improvement, and related functions;

(iv) To disclose Limited Data Sets derived from Participant Information, and information derived from such Limited Data Sets, to other [Program] Participants, for purposes of their planning, quality assessment, and related functions, and where permitted by applicable law for purposes of research; provided that the [Program] Management Committee shall serve as the Participant's agent for purposes of enforcing the provisions of Subsection 6(b) below;
(v) To disclose any Participant Information, or information derived from Participant Information, for purposes of research which has been approved by an institutional review board ("IRB"), subject to any terms and conditions to such approval;
(vi) To prepare de-identified data as provided in 45 CFR § 164.502(d); provided further that de-identified data shall not be considered Participant Information subject to this Agreement;
(vii) To disclose Participant Information if required by law, subject to the conditions of Section 3; and
(viii) To use or disclose Participant Information as otherwise necessary for legitimate purposes pertaining to performance under this Agreement.

c. [Entity] and its Subcontractors may not use or disclose Participant Information including Protected Information (as defined below) for purposes not authorized by this Agreement.

sp.02-PY.05
(viii) Limited Data Set means a set of data including Protected Information which excludes direct identifiers of the Data Subject and of the relatives, employers and household members of the Data Subject, as provided in 45 CFR § 164.514(e)(2).

sp.02-PY.05
(ix) Minimum Necessary means, for purposes of this Agreement, (A) in the case of routine and recurring types of uses or disclosures, the set of data or records which the [Program] Management Committee has established as reasonably necessary to achieve the purpose of such use or disclosure; (B) in the case of non-routine or non-recurring uses or disclosures, the set of data or records which the [Program] Management Committee determines is reasonably necessary to accomplish the purpose of the use or disclosure.

sp.02-PY.05
(xi) Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

mm.10-PY.05
Patient Privacy and Consent

General Guidelines Regarding Document Access and Use

Specify the general guidelines to be followed regarding the access and use of medical information in the XDS Affinity Domain. The Privacy Access Policies (Informative) section of the IHE BPPC Profile provides several examples of the ways this can be expressed, such as the example table below:

sp.08-PY.05
[Immunization] Registry data identifying children will not be disclosed to unauthorized individuals, including law enforcement, without the approval of the Director of the Division of Disease Control. All subpoenas, court orders, and other legal demands for [Immunization] Registry data received by any authorized user of the [Immunization]

Registry must be brought to the attention of the [Immunization] Registry Coordinator, who will consult [Program] legal counsel.

mm.06-PY.05
Authorized Users shall use the Exchange solely to access patient information in the following situations:

mm.06-PY.05
Each Network member hospital will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

If a Network member hospital, following an investigation of an alleged violation, concludes that one of its Authorized Users has inappropriately accessed information of a patient treated at that hospital, the hospital will follow its internal policies and procedures to sanction the user.

If a Network member hospital, following an investigation of an alleged violation, concludes that a user authorized by another hospital has inappropriately accessed information of a patient treated at the first hospital, the first hospital will contact the authorizing hospital and request that the authorizing hospital follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing hospital thereafter shall notify the first hospital in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first hospital concludes that the same user has inappropriately accessed patient information a second time, that hospital will request that the authorizing hospital revoke the user’s privileges to use Exchange. Any disputes between hospitals about sanctions of users will be resolved by the Exchange Task Force, whose conclusion shall be final.

If a Exchange member hospital determines that a breach has occurred, the hospital will notify Network. Network will then notify other hospitals of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their data.

Availability of Patient Information

Hospital Privacy Notices.

Each Network member hospital will include a clause in its Notice of Privacy Practices indicating that patient data may be provided to third parties in various formats. The clause shall be substantially as follows:

“In order to efficiently coordinate the treatment, payment, and health care operations aspects of your care, we may disclose your PHI in any format that we determine is secure and expeditious, e.g., verbally, electronically, via fax, and/or in paper form.”

“Para coordinar eficientemente el tratamiento, el pago, y los aspectos de la operación del cuidado de la salud, es posible que publiquemos su PHI en cualquier formato que determinamos es seguro y conveniente, por ejemplo, verbalmente, electronicamente, por medio de fax, y/o en palabra escrita.”

Each Network member hospital will allow its patients the right to prohibit the access of all their data or data from a particular encounter(s) through Exchange. Exchange will provide an option that allows hospitals to block access to a patient’s data through Exchange. If a patient has chosen this option, when a query is made about that particular patient or about electronic information to which that patient has prohibited access, Exchange will indicate "NOTE: This patient's medical record has been excluded from view in Exchange. Please contact the applicable hospital or the patient for additional details." If a patient desires to revoke or change his or her opt-out decision, the patient must contact the hospital that initially opted out the patient to make any revisions. Only the hospital that initially opted out the patient has the ability to make these revisions.

mm.06-PY.05
4. If a Network member hospital receives a request to restrict the access, use, or disclosure of patient information regarding treatment that was provided by another facility, the hospital will forward that request to the treating facility and the treating facility shall be responsible for responding to the request for restrictions.

PY.06 Agents/Subcontractors of the Participant

ph.06-PY.06
F. [State Organization] shall require that its agents, including subcontractors, to whom it provides PHI under this agreement, agree to the same restrictions and conditions that apply to [State Organization] with respect to such information.

ph.06-PY.06
9.4.4. Agents, Subcontractors. [SNO Name] shall ensure that its agents, including any subcontractor, to whom [SNO Name] provides Protected Health Information agree to the restrictions and conditions that apply to [SNO Name] with respect to such information and implement the safeguards required by Section 9.4.2 (Appropriate Safeguards) with respect to electronic Protected Health Information.

ph.06-PY.06
9.4.7 Reports. [SNO Name] shall promptly report to the Participant concerning all disclosures of Protected Health Information by [SNO Name] or any subcontractors or agents to whom it discloses Protected Health Information upon request, other than disclosures to carry out treatment, payment, and health care operations on behalf of Participant, or that are incident to such disclosures.

sp.02-PY.06
(xiv) Subcontractor means any third party to which [Entity] discloses Protected Information subject to this Agreement for purposes of providing services in connection with this Agreement.

sp.02-PY.06
(xv) Workforce means a party's employees, volunteers, trainees, and other persons under direct control of the party, including persons providing labor on an unpaid basis.

sp.02-PY.06
c. [Entity] may use Subcontractors to perform functions and activities involving Protected Information for purposes permitted by this Agreement, provided that [Entity] first obtains a written agreement from the Subcontractor requiring it to comply with privacy and information protection requirements equivalent to or more restrictive than those assumed by [Entity] under this Agreement.

sp.02-PY.06
(vi) The Participant will ensure that any agents, including any subcontractor, to whom the Participant provides the information agree to the restrictions and conditions of this Agreement applicable to the information; and

mm.09-PY.06
To not use subcontractors to perform any services described herein without prior written consent from [Program]. Participating Clinic also agrees to include provisions in its subcontracts requiring the subcontractors to comply with all applicable provisions of this Participating Clinic Agreement, including indemnifying the State, providing insurance coverage, etc.

ph.05-PY.06
To ensure that any agents, including subcontractors, to whom User or an Authorized Party provides the Limited Data Set or any part of it to agree to the same restrictions and conditions that apply to the User and Authorized Parties under this Agreement.

hh.06-PY.06
5.4 Sanctions of Users

a. Each Network will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

b. If a Network, following an investigation of an alleged violation, concludes that a user authorized by another Network inappropriately accessed information of the first Network, the first Network will contact the authorizing Network and request that the authorizing Network follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing Network thereafter shall notify the first Network in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first Network concludes that the same user has inappropriately accessed patient information a second time, that Network will request that the authorizing Network revoke the user’s privileges to use the Exchange.

c. Each Network shall require that Authorized Users notify such Network if the Authorized User determines that a breach has occurred. That Network will then notify other Networks of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their Data.

PY.07 Access to PHI; Right to Inspect and Copy

mm.07-PY.07
a. Prior to receiving a passcode or other necessary tools for accessing [State Organization], a person must have both their identity and authority verified in accordance with the procedures described below.

b. The following forms of identification are sufficient for verifying a person’s identity:

- Official and valid state ID (driver’s license, state ID card);
- Official and valid federal ID (passport, military or government ID); or
- Official and valid entity-issued picture ID.

c. The following items are sufficient for verifying a person’s authorization to access [State Organization]:

- Entity-issued ID indicating authorization to access [State Organization];
- Authorization on official entity letterhead from the Privacy Officer or other person designated to determine access levels for [State Organization]; or
- E-mail authorization from the official entity email address of the Privacy Officer or other person designated to determine access levels for [State Organization].

d. If a person provides sufficient documentation to meet the requirements of subsections (b) and (c) above, a passcode or other necessary tools for accessing [State Organization] may be issued. At the time of issuance, the person supplying the passcode or other necessary tools should place a copy of the identification and authorization documents in the designated [State Organization] Verification File.

e. If a person provides any other type of identification or authorization (student ID, court order, etc.), please contact the Privacy Officer or other person designated by this entity to determine access levels for [State Organization].

f. The majority of persons requiring access to [State Organization] should have their identification and authorization verified prior to any necessary use of the system. For this reason, emergency access to [State Organization] should not be necessary. If, however, a person requests emergency access, the entity should contact an on call provider with access to the system to assess the totality of the situation on a reasonableness basis.

Sets: Section 8.01, Section 8.02, Section 8.03, and Section 8.04. Further, with regard to [Organization]'s use of Limited Data Sets, [Organization] agrees not to identify the information or contact the Individuals whose information comprises the Limited Data Sets.

ph.06-PY.07
Limitations on Patient Access. Patient access to certain information may be limited based on a provider's determination that such information may endanger the Patient or other identifiable persons. Patient can obtain the name of the provider limiting such access, and may appeal such denial of access with provider in accordance with provider's appeal procedures.

ph.06-PY.07
You are provided with the following abilities regarding the use and disclosure of your PHI: (1) the ability to request restrictions on certain uses and disclosures of PHI, although we are not required to agree to the requested restriction; (2) the ability to receive confidential communications of PHI; (3) the ability to inspect and copy PHI, with reasonable costs of copying to apply; (4) the ability to amend PHI as allowed under HIPAA; (5) the ability to receive an accounting of disclosures of PHI; and (6) the ability to obtain a paper copy of this notice upon request.

ph.06-PY.07
G. [State Organization] agrees to comply with Provider's request to accommodate an individual's access to his/her PHI in a mutually acceptable time and manner. In the event an individual contacts [State Organization] directly about access to PHI, [State Organization] will not provide access to the individual but shall immediately forward such request to Provider.

mm.06-PY.07
The Provider will discipline, as appropriate, any person who violates the Provider's security policies and procedures and/or causes the Provider to violate the Provider Participation Agreement with [State Organization].

ph.06-PY.07
9.4.5. Inspection and Copying. [SNO Name] shall make Protected Health Information available to a Participant or any person authorized by the Participant for inspection and copying within twenty (20) days of a request by the Participant therefore.

sp.02-PY.07
d. The parties acknowledge that [Entity] has no direct relationship with Data Subjects, so that requests from Data Subjects for (i) access to, (ii) copies, (iii) amendment or (iv) an accounting of disclosures of, or (v) additional restrictions on access to Protected Information which pertains to them should be directed to the Participant. Therefore, in the event that a Data Subject or other individual contacts [Entity] in order to request any such action with respect to Protected Information which may be in or accessible through the [Program] Cardiac Registry, the [Program] Management Committee will refer the Data Subject to the Participant for an appropriate response, and shall not disclose any information directly to the individual.

sp.02-PY.07
e. Upon a request from the Participant for action with respect to Protected Information on behalf of a Data Subject, within ten (10) business days the [Program] Management Committee shall:

(i) Determine whether or not the [Program] Cardiac Registry includes a Designated Record Set (as defined in 45 CFR § 164.501) with respect to the Data Subject; if not the [Program] Management Committee shall advise the Participant accordingly and shall have no further obligation with respect to the request;
(ii) If the [Program] Cardiac Registry does include a Designated Record Set with respect to the Data Subject, the [Program] Management Committee shall advise the Participant accordingly, and provide the Participant with electronic copies of the Designated Record Set, amend the Designated Record Set, or implement additional restrictions, as requested by the Participant.

hh.06-PY.07
a. When responding to requests for release of patient information, Authorized Users shall not release data accessed or obtained through an Exchange unless required by law. Each Authorized User shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient’s medical record and the system does not maintain patient data. Each Exchange shall simply query and collate patient data from the participating providers.

hh.06-PY.07
b. Each Authorized User will follow its internal policies and procedures for responding to patients’ or patient representatives’ requests for a) access to patient information, b) amendments to the patient’s information, and c) restrictions on the access, use, or disclosure of patient information.

hh.06-PY.07
c. If an Authorized User receives a request to access or to amend patient information regarding treatment that was provided by another Authorized User, the Authorized User will forward that request to the treating provider and the treating provider shall be responsible for responding to the request for access or amendment.

sp.08-PY.07
If the parent, guardian or legal custodian chooses to exclude the child from the [Immunization] Registry that decision will be honored. The parent, guardian or legal custodian has the right to examine any data about the child contained in the [Immunization] Registry and to indicate errors in it to the provider. The provider will notify [Immunization] Registry staff of the error and note disagreement in the child's medical record.

mm.06-PY.07
a. Pursuant to the purposes specified in 45 C.F.R. §164.506(c) (the HIPAA regulations):

For treatment activities of any health care provider.

If the patient information was created at the covered entity for which the Authorized User works, for the payment or health care operations purposes of that covered entity.

If the patient information was not created at the covered entity for which the Authorized User works, for the payment activities of that covered entity, and for the health care operations activities of that covered entity, if that entity either has or had a relationship with the patient and the information is needed to conduct quality assessment and improvement activities or review the competence or qualifications of healthcare professionals.

b. Pursuant to a valid authorization when required by 45 C.F.R. §164.508 or 42 C.F.R. § 2.1, et seq., or pursuant to a valid authorization or consent when required by [State] law.

Each enrolling hospital must place appropriate restrictions on each Authorized User upon enrollment, as follows:

Exchange Physicians. Physicians with staff privileges at a Exchange hospital may have access to any patient's information when they are identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. If a Exchange physician wants access to other patients' information, a message will appear stating: "Our records indicate that you do not have an existing relationship with the patient you have selected. To continue, you agree that you need this information for the continuing care and treatment of the patient. Your access to this information is subject to audit and review." To access that patient's information, the Exchange physician must click on the "Continue" button and the override will be recorded in the audit trail.

Exchange Physician Office Staff. These individuals may have access to any patient's information only when a physician associated with that office is identified as the patient's primary, admitting, attending, consulting, or operating physician at any Network member hospital. These individuals have no override privileges to view other patients' information. However, a Network member hospital may allow at least one key member of each physician's office staff to have override privileges to view other patients' information, subject to the same audit and review process as the physicians' override privileges.

mm.06-PY.07
Exchange ED Physicians and ED Clinicians. These individuals may have access to all patient information and may access any patient information when such information is needed for the patient's continuing care and treatment, subject to the same audit and review process. Each Exchange hospital's ED clinical director or hospital clinical director shall determine which ED RNs shall have access privileges.

mm.06-PY.07
Exchange Health Care Providers. These individuals may have access only to patient information at the Exchange hospital that enrolled the user and cannot access patient information from other Exchange hospitals. These users may only view a patient's information if the enrolling hospital has created a link between the user and the patient to establish a relationship. These individuals have no override privileges to view other patients' information. These users may not search for patients at other Exchange hospitals.

mm.06-PY.07
Exchange Hospital Case Managers. These individuals may have access to any patient's information when the user is serving as a case manager for the patient and the information is needed for the continuing care and treatment of the patient. The Exchange hospital desiring to provide access to the user must establish a link between the user and a patient. These individuals have no override privileges to view other patients' information.

mm.06-PY.07
Exchange will not allow any Authorized User access to any patient information from a dedicated acute in-patient or outpatient psychiatric unit or an in-patient or outpatient substance abuse facility, as designated by each Network member hospital. Each hospital shall have the right to exclude from Exchange non-hospital patient data that is contained within its clinical information system.

mm.06-PY.07
Exchange will allow Authorized Users to access patient information from all lab results and medication histories to provide complete information for the continuing care and treatment of the patient.

mm.06-PY.07
Exchange will allow Authorized Users to access patient information dating as far back as the information is maintained on each Network member hospital's information system. Each Network member hospital shall maintain patient information on its information system for at least two years following a patient's discharge. If a Network member hospital archives certain patient data, Exchange shall access the archived data in the order specified by the hospital.

mm.06-PY.07
1. When responding to requests for release of patient information, Network member hospitals shall not release data accessed or obtained through Exchange. Each hospital shall only disclose data from its patient medical records. The information provided by Exchange does not constitute the patient's medical record and the system does not maintain patient data. Exchange simply queries and collates patient data from the participating providers.

mm.06-PY.07
2. Each Network member hospital will follow its internal policies and procedures for responding to patients' or patient representatives' requests for (a) access to patient information, (b) amendments to the patient's information, and (c) restrictions on the access, use, or disclosure of patient information.

mm.06-PY.07
3. If a Network member hospital receives a request to access or to amend patient information regarding treatment that was provided by another facility, the hospital will forward that request to the treating facility and the treating facility shall be responsible for responding to the request for access or amendment.

mm.06-PY.07
4. If a Network member hospital receives a request to restrict the access, use, or disclosure of patient information regarding treatment that was provided by another facility, the hospital will forward that request to the treating facility and the treating facility shall be responsible for responding to the request for restrictions.

sp.08-PY.07
Notification of Record Amendment. In the event a record pertaining to an individual is amended or statements pertaining to a proposed amendment of the record have been prepared for inclusion in the record, the party responsible for responding to the individual's request for amendment shall promptly provide all other parties to which it has Disclosed copies of that record with copies of the amendments or statements, as applicable. A party Receiving a copy of such amendment or statement shall promptly include it in the records maintained by that party with respect to that individual.

PY.08 Amendment of PHI

pp.06-PY.08
Section 8.06 Amendments to PHI.

Business Associate shall provide reasonable access to PHI in a Designated Record Set in the Business Associate's possession to the Covered Entity to which the PHI belongs for Covered Entity to make any amendments that Covered Entity agrees to make pursuant to 45 CFR § 164.526 or to otherwise allow Covered Entity to comply with its obligations under 45 CFR § 164.526. Amendments to PHI in the Network shall be made by Covered Entity to the Network through routine submissions of Information via an electronic interface from a system operated by the Covered Entity. Business Associate shall have no obligation to independently make such amendments or to enter such amendments into the Network. No Covered Entity shall agree to any request for an amendment without consulting with [Organization] to determine whether [Organization] and the Network are physically, administratively, and technologically capable of complying with the amendment.

pp.06-PY.08
Business Associate shall not respond directly to requests from Individual's for amendments to their PHI in a Designated Record Set. Business Associate will refer such Individuals to the relevant Covered Entity so that the Covered Entity can coordinate and prepare a timely response to the Individual.

ph.06-PY.08
You are provided with the following abilities regarding the use and disclosure of your PHI: (1) the ability to request restrictions on certain uses and disclosures of PHI, although we are not required to agree to the requested restriction; (2) the ability to receive confidential communications of PHI; (3) the ability to inspect and copy PHI, with reasonable costs of copying to apply; (4) the ability to amend PHI as allowed under HIPAA; (5) the ability to receive an accounting of disclosures of PHI; and (6) the ability to obtain a paper copy of this notice upon request.

ph.06-PY.08
H. [State Organization] agrees to comply with Provider's request to make amendments to PHI pursuant to 45 C.F.R. 164.526. [State Organization] shall promptly incorporate any such amendments into the PHI. In the event an individual contacts [State Organization] directly about making amendments to PHI, [State Organization] will not make any amendments to the individual's PHI, but shall forward such request to Provider.

ph.06-PY.08
9.4.6. Amendments. [SNO Name] shall make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information requested by the Participant.

sp.02-PY.08
d. The parties acknowledge that [Entity] has no direct relationship with Data Subjects, so that requests from Data Subjects for (i) access to, (ii) copies, (iii) amendment or (iv) an accounting of disclosures of, or (v) additional restrictions on access to Protected Information which pertains to them should be directed to the Participant. Therefore, in the event that a Data Subject or other individual contacts [Entity] in order to request any such action with respect to Protected Information which may be in or accessible through the [Program] Cardiac Registry, the [Program] Management Committee will refer the Data Subject to the Participant for an appropriate response, and shall not disclose any information directly to the individual.

sp.02-PY.08
e. Upon a request from the Participant for action with respect to Protected Information on behalf of a Data Subject, within ten (10) business days the [Program] Management Committee shall:

(i) Determine whether or not the [Program] Cardiac Registry includes a Designated Record Set (as defined in 45 CFR § 164.501) with respect to the Data Subject; if not the [Program] Management Committee shall advise the Participant accordingly and shall have no further obligation with respect to the request;
(ii) If the [Program] Cardiac Registry does include a Designated Record Set with respect to the Data Subject, the [Program] Management Committee shall advise the Participant accordingly, and provide the Participant with electronic copies of the Designated Record Set, amend the Designated Record Set, or implement additional restrictions, as requested by the Participant.

hh.06-PY.08
b. Each Authorized User will follow its internal policies and procedures for responding to patients' or patient representatives' requests for (a) access to patient information, (b) amendments to the patient's information, and (c) restrictions on the access, use, or disclosure of patient information.

hh.06-PY.08
c. If an Authorized User receives a request to access or to amend patient information regarding treatment that was provided by another Authorized User, the Authorized User will forward that request to the treating provider and the treating provider shall be responsible for responding to the request for access or amendment.

mm.06-PY.08
2. Each Network member hospital will follow its internal policies and procedures for responding to patients' or patient representatives' requests for (a) access to patient information, (b) amendments to the patient's information, and (c) restrictions on the access, use, or disclosure of patient information.

mm.06-PY.08
3. If a Network member hospital receives a request to access or to amend patient information regarding treatment that was provided by another facility, the hospital will

forward that request to the treating facility and the treating facility shall be responsible for responding to the request for access or amendment.

sp.08-PY.08
Notification of Record Amendment. In the event a record pertaining to an individual is amended or statements pertaining to a proposed amendment of the record have been prepared for inclusion in the record, the party responsible for responding to the individual's request for amendment shall promptly provide all other parties to which it has Disclosed copies of that record with copies of the amendments or statements, as applicable. A party Receiving a copy of such amendment or statement shall promptly include it in the records maintained by that party with respect to that individual.

sp.08-PY.08
Disclosure Records. Maintain a record of all Disclosures made of Protected Information, including (a) the date of the Disclosure, (b) the name and address of the organization and/or individual Receiving the Information; (c) a brief description of the information Disclosed; (d) if the Disclosure was not to the Individual, the Purpose for the Disclosure; and (e) a copy of all requests for Disclosures ("Disclosure Accounting").

sp.08-PY.08
Information Ownership.

The following provisions control the ownership of information Disclosed under this Agreement. These provisions shall not apply to information which (a) is readily available or can be readily ascertained through public sources, (b) a party has previously Received from a source or sources legally entitled to Disclose such Information to the party, or (c) can be demonstrated by documentation to have been independently developed by the Receiving Party without reference to any information provided by the Disclosing Party.

Information Presumed Owned by Disclosing Party. All information shall be deemed to be the exclusive property of the Disclosing Party, unless (a) otherwise expressly agreed in Writing or (b) the information was previously Received by the Disclosing Party from another party to this Agreement, who did not disclaim ownership in Writing.

PY.09 Reports of Disclosure of PHI

pp.06-PY.09
Section 8.07 Documentation and Provision of Disclosures.

(a) Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Such documentation shall be kept with regard to all disclosures of PHI except for the disclosures that are excepted from the accounting requirement at 45 CFR § 164.528(a) (as it may be amended from time to time), which currently include the following:

- To carry out treatment, payment, and health care operations as provided in 45 CFR § 164.506;
- To Individuals of PHI about them as provided in 45 CFR § 164.502;
- Incident to a use or disclosure otherwise permitted or required by the Privacy Rule, as provided by 45 CFR § 164.502;
- Pursuant to an authorization by an Individual as provided in 45 CFR § 164.508;

- For Covered Entity's facility directory or to persons involved in an Individual's care or other notification purposes as provided in 45 CFR § 164.510;
- For national security or intelligence purposes as provided in 45 CFR § 164.512(k)(2);
- To correctional institutions or law enforcement officials as provided in 45 CFR § 164.512(k)(5);
- As part of a Limited Data Set in accordance with 45 CFR § 164.514(e); or
- That occurred prior to April 14, 2003.

pp.06-PY.09
For each non-excepted disclosure, Business Associate shall document the following information: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably states the basis for the disclosure.

pp.06-PY.09
Business Associate shall provide to a requesting Covered Entity, within a reasonable time period after Covered Entity's request, information collected in accordance with this Section, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. However, Business Associate shall not respond directly to requests from Individual's for an accounting of disclosures. Business Associate will refer such Individuals to the relevant Covered Entity so that the Covered Entity can coordinate and prepare a timely response to the Individual.

ph.06-PY.09
You are provided with the following abilities regarding the use and disclosure of your PHI: (1) the ability to request restrictions on certain uses and disclosures of PHI, although we are not required to agree to the requested restriction; (2) the ability to receive confidential communications of PHI; (3) the ability to inspect and copy PHI, with reasonable costs of copying to apply; (4) the ability to amend PHI as allowed under HIPAA; (5) the ability to receive an accounting of disclosures of PHI; and (6) the ability to obtain a paper copy of this notice upon request.

ph.06-PY.09
D. If [State Organization] becomes aware of any use or disclosure of PHI, not provided for by this Agreement, it shall report such use or disclosure to Provider.

ph.06-PY.09
I. [State Organization] agrees to document such disclosures of PHI and information related to such disclosures as would be required for Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528. [State Organization] agrees to provide to Provider in a mutually acceptable time and manner, information collected in accordance with this section, to permit Provider to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528.

ph.06-PY.09
Provider agrees to regularly monitor and audit access to [State Organization] and report any issues to [State Organization] upon discovery. Provider shall immediately notify [State Organization] of the revocation of an individual's access and will provide a follow-up report regarding the breach/violation within sixty (60) days of such breach/violation.

ph.06-PY.09
9.3 Reporting of Serious Breaches. Provisions requiring the SNO and Participant to report to each other concerning serious breaches of confidentiality of patient health information. Without limiting Section 9.4.7(Reports), if applicable to [SNO Name], [SNO Name] and Participant shall report to the other any serious use or disclosure of Protected Health Information not provided for by the Terms and Conditions of which [SNO Name] or Participant becomes aware, and any security incident concerning electronic Protected Health Information (a "Serious Breach of Confidentiality or Security"). A "Serious Breach of Confidentiality or Security" is one that adversely affects (a) the viability of the NHIN; (b) the trust among Participants or (c) the SNO's legal liability.

ph.06-PY.09
9.4.1 Use and Disclosure. [SNO Name] shall use and disclose Protected Health Information only for the purposes of [SNO Name]'s performance of its responsibilities described in the Terms and Conditions. Without limiting the foregoing, [SNO Name] may use and disclose Protected Health Information for the proper management and administration of [SNO Name]'s business and to carry out its own legal responsibilities; provided, that any disclosure pursuant to this Section 9.4.1 (Use and Disclosure) shall either be required by law or be made with reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to such person, and that the person will notify [SNO Name] of any instances of which it is aware in which the confidentiality of the information has been breached.

ph.06-PY.09
9.4.3. Reports to Participant. [SNO Name] shall report to the Participant any use or disclosure of Protected Health Information of the Participant not provided for by the Terms and Conditions of which [SNO Name] becomes aware, and any security incident concerning electronic Protected Health Information.

ph.06-PY.09
9.4.7 Reports. [SNO Name] shall promptly report to the Participant concerning all disclosures of Protected Health Information by [SNO Name] or any subcontractors or agents to whom it discloses Protected Health Information upon request, other than disclosures to carry out treatment, payment, and health care operations on behalf of Participant, or that are incident to such disclosures.

ss.05-PY.09
Signatories will endeavor to notify a sending signatory, at the earliest possible time, if a request for health data provided by that jurisdiction is made under the receiving signatory's Freedom of Information Act or the equivalent of such an act under that jurisdiction's law, or the receipt of a subpoena.

sp.02-PY.09
f. Upon request by the Participant, within ten (10) business days the [Program] Management Committee shall provide an Accounting of Disclosures with respect to any identified Data Subject with respect to whom [Entity] has disclosed Protected Information; provided that:

(i) [Entity] shall have no obligation to track or account for disclosures of Protected Information which are made for purposes of Health Care Operations or as part of a Limited Data Set.

(ii) Any such Accounting for Disclosures shall include (a) the disclosure date, (b) the name and (if known) address of the person or entity to whom the disclosure was made, (c) a brief description of the Protected Information disclosed, and (d) a brief statement of the purpose(s) of the disclosure.

sp.02-PY.09
(i) Accounting of Disclosures means an accounting to a Data Subject of all disclosures made of PHI pertaining to that Individual.

mm.06-PY.09
Audit Trails AO.03/mm.06/(SII(C) – Exchange will record each time an Authorized User accesses the Exchange and will record every item of patient information accessed by the Authorized User.

The audit trail will identify whether the Authorized User "overrode" the system to access information of patients with whom the user does not have a pre-existing relationship. Since ED clinicians and ED physicians are not required to have a pre-existing relationship with a patient, their overrides are not recorded in the audit trail.

Each Network member hospital routinely will review the audit trails of information accessed from its facility to identify and investigate any potential abuses or violations of the Exchange Policies and Procedures or applicable federal or state laws or regulations.

mm.06-PY.09
Upon request, each Network member hospital will follow its internal policies and procedures for providing an accounting of disclosures to the patient or patient's representative requesting the accounting, in order to indicate who has accessed the patient's information for treatment provided at that member hospital's system.

mm.06-PY.09
2. Each Network member hospital will follow its internal policies and procedures for responding to patients' or patient representatives' requests for a) access to patient information, b) amendments to the patient's information, and c) restrictions on the access, use, or disclosure of patient information.

sp.08-PY.09
Provision of Information and Amendment of Records. Maintain procedures for the Providing Disclosure Accountings directly to Individuals, or to Disclosing Parties who have been requested to provide a Disclosure Accounting

sp.08-PY.09
Communication of amendments or information pertaining to amendments of Protected Information by Individuals from Disclosing Parties to Receiving Parties;[15] and PY.08

Including amendments or information pertaining to amendments of Protected Information Received from Individuals or Disclosing Parties, into record sets of Protected Information.

[15] See Privacy Rule at 82,825, 45 CFR sec. 164.526(c)(3).

PY.10 Availability of Records to HHS

ph.06-PY.10
J. [State Organization] shall make its internal practices, books and records relating to uses and disclosures of PHI available to the Secretary of the U.S. Department of Health and Human Services or designee, for purposes of determining Provider and [State Organization] compliance with the Privacy Rule.

ph.06-PY.10
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network) to have access to his/her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.
- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-PY.10
Providing customized summary reports with non-identifying data or statistics as needed for public health or other governmental purposes required by law.

ph.06-PY.10
9.4.8. Availability of Records. [SNO Name] shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the United States Department of Health and Human Services, for purposes of determining the Participant’s compliance with its legal obligations.

sp.02-PY.10
j. The [Program] Management Committee shall retain records of its policies and procedures, Subcontractor contracts, Accountings of Disclosures, communications with Data Subjects, security incident reports, and other documentation material to its compliance with this Section 4, for a period of no less than six (6) years from the later of the date on which it was created or the last date on which the document was effect (if applicable).

sp.02-PY.10
k. [Entity] shall make its internal practices, books and records pertaining to the use and disclosure of Protected Information received from, or created or received by [Entity] on behalf of the Participant available to HHS for purposes of determining the Participant’s compliance with HIPAA upon request.

sp.02-PY.10
5. Medicare Compliance Record Access.

If required for purposes of 45 CFR §§ 420.300 – 420.320, upon written request [Entity] shall make this Agreement and any other necessary books, records and documents available to HHS or the Comptroller General or their duly authorized representatives, for purposes of verifying the nature and extent of any costs incurred by the Participant for services furnished by [Entity] for which payment may be or have been made under Medicare, Medicaid or other applicable federal reimbursement programs.

[Entity] shall require any subcontractor which (a) is a related organization (as defined in 42 CFR § 420.301) and (b) carries out any of the duties of [Entity] under this Agreement by providing services of a value or cost of ten thousand dollars ($10,000.00) or more in any twelve (12) period, to provide similar access to HHS, the Comptroller General or their duly authorized representatives.

[Entity]'s obligation to provide access to records under this Section 5 shall extend for four (4) years from the last date on which services are provided under this Agreement, and survive the termination of this Agreement for such period if applicable.

hh.06-PY.10
Each Network or Authorized User shall maintain patient information on its information system for the minimum amount of time required by law but in no event less than six (6) years following a patient's discharge or treatment.

PY.11 Survival of Privacy Provisions after Termination of Agreement with the HIE

pp.06-PY.11
Section 12.05 Infeasibility of Return of Information. The Parties recognize that due to the interconnectivity of the Network and the fact that the Participants will be relying on the Information on the Network to make Treatment decisions for patients, it is necessary for the Information to remain on the Network for potential risk management and legal defense purposes. Therefore, it is infeasible for Information to be returned or destroyed at the termination of the Agreement or the withdrawal of a Participant. However, if elected in compliance with, or mandated by a term of, this Article, Information may no longer be available for Participants to access after the termination of this Agreement or the withdrawal of a Participant except for the purposes that make the return or destruction of the Information infeasible. [Organization] shall continue to store the Information on the Network subject to the confidentiality obligations in this Agreement and shall not further use or disclose the Information except as allowed by this Agreement, including, but not limited to, the reasons set forth above that make the return or destruction infeasible.

ph.06-PY.11
K. Upon termination of this Agreement, [State Organization] shall return or destroy all PHI and will retain no copies of such information. If such return or destruction of PHI is not feasible, [State Organization] agrees that the provisions of this Agreement are extended beyond termination to such PHI, and [State Organization] shall limit all further uses and disclosures to those purposes that make the return or destruction of such PHI infeasible.

ph.06-PY.11
Survival of Obligation. Articles III, VIII and X of this Agreement shall survive the expiration or termination of this Agreement.

ph.06-PY.11
4.11 Survival of Provisions. The provisions of the Registration Agreement that shall continue to bind the Participant following termination. The following provisions of the Terms and Conditions shall survive any termination of a Participant's Registration Agreement: Section 5.5 (Responsibility for Conduct of Participant and Authorized Users), Section 9

(Protected Health Information), Section 13 (Proprietary Information), Section 14.8 (Limitation on Liability) and Section 15.2.1 (Indemnification).

ph.06-PY.11
9.4.9. Action Upon Termination. Given the role of the System and the NHIN, the destruction or return to the Participant of Protected Health Information following the termination of the Participant's Registration Agreement would be infeasible. Therefore, upon termination of the Participant's Registration Agreement, [SNO Name] shall extend the protections of this Section 9.4 (Business Associate Agreement) to such information, and shall limit further use and disclosure of the information to those purposes that make the return or destruction of the information infeasible.

sp.02-PY.11
i. The Participant acknowledges that the purposes for which Participant Information is provided under this Agreement may make the return or destruction of all Protected Information included in such Participant Information or information derived from Participant Information not feasible, and agrees that [Entity] shall have no obligation to return or destroy such information upon the termination of this Agreement, provided that it shall remain protections of this Agreement and shall only be used for those purposes authorized by this Agreement which make the return or destruction of the information infeasible.

sp.02-PY.11
l. The provisions of this Subsections 4(i) – 4(k) shall survive the termination of this Agreement for a period of six (6) years from the date of termination or six (6) years from the last date on which [Entity] retains any Protected Information received from or on behalf of the Participant, whichever comes first.

PY.12 Miscellaneous Privacy Provisions

pp.06-PY.12
Section 8.11 Notice of Privacy Practices. Each Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any changes to such notice. Each Covered Entity shall ensure that its Notice of Privacy Practices includes provisions that adequately inform Individuals: (a) that their PHI may be used and disclosed and received from other health care providers for Treatment purposes; (b) of the research uses and disclosures of PHI set forth in this Agreement; and (c) that their PHI may be used and disclosed by Business Associate to perform functions like those allowed in this Agreement.

pp.06-PY.12
Section 8.13 Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure in violation of the requirements of this Agreement.

pp.06-PY.12
Section 8.08 Availability of Internal Practices, Books and Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, a Covered Entity available to the Secretary, in a reasonable time and manner designated by the Secretary, for purposes of determining a Covered Entity's compliance with the Privacy Rule.

pp.06-PY.12
Section 8.09 Change or Revocation of Permission. Each Covered Entity shall provide Business Associate with notice of any changes in, or revocation of, permission by an Individual to use or disclose PHI, or of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR § 164.522, if such changes or restrictions affect a Business Associate's permitted or required uses and disclosures. A Covered Entity shall not agree to any such changes or restrictions without consulting with [Organization] to determine whether [Organization] and the Network are physically, administratively, and technologically capable of complying with such changes or restrictions, and without obtaining [Organization]'s consent (which will not be unreasonably withheld). No Business Associate shall be responsible for any use or disclosure that fails to comply with any such change or revocation that occurs prior to being notified by the Covered Entity pursuant to this Section.

sp.09-PY.12
Model informed consent provisions

pp.05-PY.12
VI. The Insurer acknowledges that under its contracts with health care providers [Entity] has guaranteed that it will not release any information identifying any provider, or any individual affiliated with any provider under contract with [Entity], to any third party, including but not limited to insurers, without the written consent of the provider or other identified person(s), unless such disclosure is otherwise required by law. Nothing in this Agreement shall be construed as imposing any obligation on [Entity] to fail to comply with that guarantee.

ph.06-PY.12
I acknowledge that I have received a copy of the [State Organization] Notice of Privacy Practices attached hereto as Exhibit A. I further acknowledge that should the Privacy Notice change, I may obtain a revised notice by contacting visiting the [State Organization] website.

ph.06-PY.12
There may be times when we would like to release your PHI for other reasons. At those times, and before we disclose it, we will ask you to provide us with written authorization. Written authorizations may be revoked at any time, except to the extent that we have already taken action in reliance upon the authorization, or if the authorization was obtained as a condition of obtaining insurance coverage, in which case the insurer has the right to contest a claim under the policy.

ph.06-PY.12
If you believe these privacy rights have been violated, you may file a written complaint with the [State Organization] Privacy Officer or the Department of Health and Human Services. No retaliation will occur against you for filing a complaint.

ph.06-PY.12
E. [State Organization] shall mitigate, to the extent reasonable practicable, any deleterious effects from any improper use and/or disclosure of PHI that [State Organization] reports to Provider.

mm.06-PY.12
Provider personnel must take reasonable steps to protect the privacy of all verbal exchanges or discussions involving PHI (regardless of where the discussion occurs) by following appropriate Provider policies and procedures.

It is understood that in certain work environments Uses or Disclosures that are incidental to an otherwise permitted Use or Disclosure may occur, and such incidental Uses or Disclosures are not considered a violation provided that Provider has met the reasonable safeguards and minimum necessary requirements (if applicable).

ph.06-PY.12
9.4.10 Special Termination. Notwithstanding any other provision of the Terms and Conditions to the contrary, the Participant may immediately terminate its Registration Agreement if it determines that [SNO Name] has violated a material term of this Section 9.4 (Business Associate Agreement), and [SNO Name] fails to remedy the violation within thirty (30) days following receipt of written notice thereof.

sp.02-PY.12
(vi) The Participant will not identify the Data Subjects to whom the information pertains, or contact those Data Subjects.

sp.02-PY.12
[Entity] or the [Program] Management Committee may use information from the [Program] Cardiac Registry which does not identify the Participant and/or its associated Providers for general educational purposes and to satisfy contractual reporting requirements, as authorized by the [Program] Management Committee.

4. Information Protection Law Compliance.

a. The following definitions shall apply to terms capitalized in this Agreement:

mm.10-PY.12
Patient consent

The rules for patient consent have to be harmonized or agreements have to be defined on how differences shall be bridged when harmonization is not possible. Both parties shall agree to this in the Policy Agreement.

mm.10-PY.12
Patient privacy is a key issue in trans-border information exchange**.**

mm.10-PY.12
In order to gain a patient's full confidence with the information transactions it is of utmost importance that the rules are clear and easily understood by the patients**.**

mm.10-PY.12
Specify whether or not support of the IHE XDS Basic Patient Privacy Consents Content Profile is mandatory or not for systems connecting to this XDS Affinity Domain**.**

mm.10-PY.12
Define the rules for the use of BPPC in the XDS Affinity Domain. Refer to the IHE ITI BPPC Profile for a thorough discussion of these rules. Some examples of the rules to define are:

- Where are the set of common consent agreements going to be published.

- How are the Policy OIDs going to be distributed to and used by systems in the XDS Affinity Domain.
- The configuration of the Document Consumers and Sources on the appropriate behaviors when specific consent OIDs are used or referenced.
- Document Sources should select the appropriate OIDs when documents are published.
- Document Consumers should enforce the policies associated with the OIDs when documents are queried and retrieved.

mm.10-PY.12
Specify if on a patient by patient basis Consent documents will be published into the XDS Affinity Domain.

If Consent documents are published then specify whether "wet" signatures (thus requiring support for XDS Scanned Documents), or electronic patient consents will be used.

If "wet" signatures are used then specify whether or not the Scanned Documents must be digitally signed or not.

If electronic patient consents are used then define how the certificates are obtained for the patient digital signatures.

Note that in XDS Affinity Domains where implied consent is used, Consent documents are not likely to be published**.**

mm.10-PY.12
Define all the conditions that can be used for defining a patient's privacy consent (type of data, type of access, etc.).

mm.10-PY.12
Privacy Override Guidelines

This section should specify those conditions (emergency mode, break-glass, system failure mode, etc) under which privacy restrictions can be over-ridden. This should specify any special procedures that must be followed and how such cases of privacy override must be documented and reviewed.

mm.10-PY.12
Correction Policy (Modify)

Update Policy (Modify)

Document Read Policy

Document Deletion Policy

Folder Policy

Explain any XDS Affinity Domain specific policies regarding Folders.

Ethics

The rules and regulations will never cover all possible situations. Therefore ethics have to be taken into consideration and a memorandum has to be formulated to give everybody a good understanding about the framework for responsibility that everyone has to work within.

ph.06-PY.12
Hospital shall provide its employees who are granted Data User Accounts with education and training on HIPAA requirements to maintain the confidentiality of patient information accessed through Exchange.

sp.08-PY.12
Policies, Consents and Authorizations. If a party is required or elects to publish a consent and/or authorization forms, and/or a privacy policy or policies, the party shall (a) ensure that such documentation and/or the policy does not conflict with the party's ability to perform its obligations under this Agreement, and (b) provide copies of such documentation to all other parties to this Agreement on or before their publication to Individuals.

sp.08-PY.12
Additional Privacy Protections at Individual Request. In the event a Disclosing Party has agreed to provide additional privacy protections to information pertaining to an individual, the Disclosing Party shall notify the Receiving Party on the date such information is Transmitted to the Receiving Party or the date on which the Disclosing Party makes such an agreement, whichever is later. In the event or an individual has revoked an authorization or consent to disclosure of information previously given to the Disclosing Party, which pertains to information Disclosed to a Receiving Party, the Disclosing Party shall promptly notify the Receiving Party of such revocation, and the Receiving Party shall implement such processes and procedures as may be necessary to implement such revocation.

4.8 Security (SE)

SE.01 Compliance with HIPAA Security Generally

sp.08-SE.01
Protecting the privacy of patients and the security of information contained in the [Immunization] Registry is a high priority for the [City] Department of Public Health

sp.03-SE.01
Abide by the rules and regulations set forth in 45 CFR Parts 160 and 164 (HIPAA) as Participating Clinic is a "covered entity" as defined in the Health Insurance Portability and Accountability Act, 45 CFR § 160.103.

ph.02-SE.01
Appropriate Safeguards to Prevent Unauthorized Use or Disclosure of Data. RESEARCHER and any contractor authorized by RESEARCHER under this Agreement shall effect, implement and maintain reasonable and appropriate safeguards for the protection of data subject to this Agreement, at all times while such data subject to this Agreement is subject to their possession or control. These safeguards shall include the following:

ph.02-SE.01
a. Policies and procedures to prevent any use or disclosure of data subject to this Agreement, contrary to the requirements of this Agreement.

ss.07-SE.01
All records are considered confidential and covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ss.07-SE.01
All records are considered confidential and covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

ph.06-SE.01
Compliance with Law. [State Organization] shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which [State Organization] reasonably believes: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally-funded healthcare program, including the Medicare and Medicaid programs.

ph.06-SE.01
[State Organization] will use appropriate administrative, technical and physical safeguards to protect the confidentiality and integrity of PHI and to prevent the use or disclosure of any individually identifiable health information received from or on behalf of Provider other than as permitted or required by Federal or State law or by this Agreement. [State Organization] agrees to comply with applicable requirements of law relating to PHI and with respect to any task or other activity [State Organization] performs on behalf of Provider to the extent that the Provider would be required to comply with such requirements.

ph.06-SE.01
9.4.2 Appropriate Safeguards. [SNO Name] shall use appropriate safeguards to prevent use or disclosure of Protected Health Information otherwise than as permitted by the Terms and Conditions, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of that Protected Health Information.

mm.06-SE.01
To ensure that all users of the Provider's systems fully comply with the Security Policies and Procedures, the Provider will discipline and sanction such users, as appropriate, for any violation of the Security Policies in accordance with the following:

A. General Rule.

The Provider shall apply appropriate sanctions against any person that fails to comply with the Provider's Security Policies and Procedures.

The type and severity of sanction applied shall be in accordance with the Provider's Privacy and Security Policies and Procedures.

Employees, agents, and other contractors should be aware that violations of a severe nature may result in notification by [State Organization] to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.

mm.06-SE.01
Provider personnel must ensure that workstations are equipped with reasonable security measures so that unauthorized persons cannot access [State Organization] on an unattended workstation or through the Provider's server or network.

ph.09-SE.01
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security.

ph.06-SE.01
5.6 Termination of Authorized Users.

How the SNO will assure that Participants perform their responsibilities to control the acts of Authorized Users.

Participant shall require that all of its Authorized Users use the System and the Services only in accordance with the Terms and Conditions, including without limitation those governing the confidentiality, privacy and security of protected health information. Participant shall discipline appropriately any of its Authorized Users who fail to act in accordance with the Terms and Conditions in accordance with Participant's disciplinary policies and procedures.

ph.06-SE.01
5.3 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users. Based on the information provided by the Participant pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

ph.06-SE.01
9.4.2 Appropriate Safeguards. [SNO Name] shall use appropriate safeguards to prevent use or disclosure of Protected Health Information otherwise than as permitted by the Terms and Conditions, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of that Protected Health Information.

sp.02-SE.01
(v) HIPAA Security Rule means the regulations issued by HHS codified at 45 CFR Part 164.

hh.06-SE.01
Each Network shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

sp.08-SE.01
Only personnel whose assigned duties include functions associated with the immunization of children can be given access to Registry information. All personnel including permanent and temporary employees, volunteers, contractors, and consultants will be required to sign a [Immunization] Registry User Security and Confidentiality Agreement before gaining access to the Registry. Whenever a user terminates the employment or other status, that person's [Immunization] Registry user account must be removed immediately. A user taking an extended leave of absence must have the account status set to Inactive. Users who fail to access the [Immunization] Registry for more than 60 consecutive days will have their accounts inactivated by [Immunization] Registry.

ph.06-SE.01
Hospital shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on Hospital's computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from Hospital's facility using the Exchange. Hospital shall report to the relevant Data Provider any use or disclosure of Data created at that Data Provider of which Hospital becomes aware that is not permitted or required by this Agreement or by law.

sp.08-SE.01
If the information is Transmitted electronically, the Disclosing Party shall use or maintain technological systems and procedures to guard against unauthorized access to information that is Transmitted electronically, including encryption and/or appropriate technical security mechanisms.

sp.08-SE.01
Computer System Administration. In the event the parties have implemented Transmission procedures under which the Disclosing Party has the capacity to directly access a computer or computer systems of the Receiving Party, the Disclosing Party shall:[16]

Maintain a designated individual or individuals to serve as security officer(s) responsible for supervising the security of the Disclosing Party's applications permitting access to the Receiving Party's systems, who shall further be responsible for communicating with the Receiving Party with respect to matters affecting the security of the Receiving Party's computer or computer systems.[17]

SE.02 Breach of Security

mm.06-SE.02
Each Network member hospital will follow its internal policies and procedures to sanction its Authorized Users who inappropriately access patient information from the Exchange.

If a Network member hospital, following an investigation of an alleged violation, concludes that one of its Authorized Users has inappropriately accessed information of a patient treated at that hospital, the hospital will follow its internal policies and procedures to sanction the user.

[16] The following provisions are intended to establish "chain of trust" obligations applicable to a Disclosing Party under the Draft Security Rule. A Covered Entity will in any case have to comply with all the HIPAA security requirements.

[17] While a security officer is not specifically required, security management processes including oversight and accountability are required under the Draft Security Rule at 43,267, 45 CFR 142.308(a)(10) and .308(b)(1).

If a Network member hospital, following an investigation of an alleged violation, concludes that a user authorized by another hospital has inappropriately accessed information of a patient treated at the first hospital, the first hospital will contact the authorizing hospital and request that the authorizing hospital follow its internal policies and procedures to investigate the apparent violation and, if appropriate, sanction the user. The authorizing hospital thereafter shall notify the first hospital in writing that it has concluded its investigation, determined that a violation did or did not occur, and taken appropriate action without specifying the particular action taken. If the first hospital concludes that the same user has inappropriately accessed patient information a second time, that hospital will request that the authorizing hospital revoke the user's privileges to use Exchange. Any disputes between hospitals about sanctions of users will be resolved by the Exchange Task Force, whose conclusion shall be final.

If a Exchange member hospital determines that a breach has occurred, the hospital will notify Network. Network will then notify other hospitals of the breach and suggest that they conduct an audit to determine if the breaching party inappropriately accessed their data.

hh.06-SE.02
Each Network shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

sp.02-SE.02
(xiii) Security Incident means any action or event which:

A. Provides an unauthorized person with access to and/or the ability to use, disclose, modify or destroy Protected Information;

B. Permits an unauthorized person to modify the functioning of an information system, including any equipment or device and any software application or operating system which is a component of an information system; or

C. Involves the acquisition of more than the Minimum Necessary Protected Information by a Subcontractor or member of [Entity]'s Workforce.

ph.06-SE.02
9.4.3. Reports to Participant. [SNO Name] shall report to the Participant any use or disclosure of Protected Health Information of the Participant not provided for by the Terms and Conditions of which [SNO Name] becomes aware, and any security incident concerning electronic Protected Health Information.

mm.06-SE.02
To ensure that all users of the Provider's systems fully comply with the Security Policies and Procedures, the Provider will discipline and sanction such users, as appropriate, for any violation of the Security Policies in accordance with the following:

A. General Rule.

The Provider shall apply appropriate sanctions against any person that fails to comply with the Provider's Security Policies and Procedures.

The type and severity of sanction applied shall be in accordance with the Provider's Privacy and Security Policies and Procedures.

Employees, agents, and other contractors should be aware that violations of a severe nature may result in notification by [State Organization] to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.

ph.06-SE.02
[State Organization] agrees to regularly monitor and audit the access of each Network participant, and to take reasonable steps to pursue any breach or other privacy and security issues raised by such monitoring and auditing.

ph.06-SE.02
Provider agrees to regularly monitor and audit access to [State Organization] and report any issues to [State Organization] upon discovery. Provider shall immediately notify [State Organization] of the revocation of an individual's access and will provide a follow-up report regarding the breach/violation within sixty (60) days of such breach/violation.

sp.09-SE.02
Facilitate the evaluation of the level of data sensitivity and the levels of access controls the institution will require for each data set to be shared.

pp.05-SE.02
If [Entity] has reason to believe that the Insurer may have permitted a material breach of these Procedures to Maintain Enrollee Privacy, or from time to time as part of [Entity]'s Privacy Compliance Plan, [Entity] may audit the Insurer to determine its compliance with these Procedures. The Insurer will cooperate with any such audit, which will be at [Entity]'s expense after giving reasonable notice to the Insurer, and conducted with as little disruption of Insurer's business as reasonably possible. All information reviewed by [Entity] for audit purposes will be kept confidential under the terms of [Entity]'s Obligation to Maintain Insurer Confidentiality, unless [Entity] reasonably believes disclosure is necessary to establish a claim or defense on behalf of [Entity] in a legal proceeding involving [Entity] and the Insurer.

pp.05-SE.02
If [Entity] has reason to believe that the Provider may have permitted a material breach of these Obligations to Maintain Patient Privacy, or from time to time as part of [Entity]'s Privacy Compliance Plan, [Entity] may audit the Provider to determine its compliance with these Obligations. The Provider will cooperate with any such audit, which will be at [Entity]'s expense after giving reasonable notice to the Provider, and conducted with as little disruption of Provider's business as reasonably possible. All information reviewed by [Entity] for audit purposes will be kept confidential under the terms of [Entity]'s Obligation to Maintain Provider Confidentiality, unless [Entity] reasonably believes disclosure is necessary to establish a claim or defense on behalf of [Entity] in a legal proceeding involving [Entity] and the Provider.

mm.06-SE.02
Process for Responding to Possible Violations.

Persons affiliated with the Provider, regardless of whether they have access to [State Organization], are encouraged to report possible breaches of confidentiality to the Provider's Privacy Officer.

The Provider shall respond to possible violations in accordance with the Provider's Security Policies and Procedures and general procedures for violation of Provider policy. The name of any persons involved with the possible violation shall be reported to [State Organization] within ten (10) days of the discovery of the violation.

A record of the event and any discipline imposed shall be maintained in the employee's personnel file with a copy to be filed in a master file maintained by the Privacy Officer, and to be provided to [State Organization] within sixty (60) days of the event.

Appropriate Provider personnel are responsible for determining the severity of sanctions necessary, in accordance with Provider policies and procedures. A record of the final determination shall be maintained by Provider, to be provided to [State Organization] within sixty (60) days of the determination.

pp.05-SE.02
If [Entity] has reason to believe that the Provider may have permitted a material breach of these Obligations to Maintain Patient Privacy, or from time to time as part of [Entity]'s Privacy Compliance Plan, [Entity] may audit the Provider to determine its compliance with these Obligations. The Provider will cooperate with any such audit, which will be at [Entity]'s expense after giving reasonable notice to the Provider, and conducted with as little disruption of Provider's business as reasonably possible. All information reviewed by [Entity] for audit purposes will be kept confidential under the terms of [Entity]'s Obligation to Maintain Provider Confidentiality, unless [Entity] reasonably believes disclosure is necessary to establish a claim or defense on behalf of [Entity] in a legal proceeding involving [Entity] and the Provider.

Agreement (including any renewal period) and that are documented through generally accepted accounting methods; or

hh.06-SE.02
Each Network shall assure that each Authorized User shall report to the relevant Authorized User and the Network any use or disclosure of Data created at that Authorized User of which the Registered User becomes aware that is not permitted or required by this Agreement or by law.

sp.02-SE.02
[Entity] shall promptly report any confirmed Security Incident affecting Participant Information in the [Program] Cardiac Registry to the Participant, unless prohibited from doing so by any law enforcement, homeland security or national defense agency. The Participant shall have primary responsibility for notification of Data Subjects potentially affected by a confirmed Security Incident, if such notification is required by law or elected by the Participant; provided that [Entity] may give such notification if [Entity] determines that it is required by law and the Participant fails or declines to give it. Notification by the Participant shall be deemed notification by [Entity] and [Entity] shall be identified as a notifying party, if [Entity] determines that notification by [Entity] is or may be required by law.

ph.05-SE.02
To report to The Regents, through the Health System Privacy Officer, any use or disclosure of the Limited Data Set or any part of it not provided for by this Agreement of which User or any Authorized Party becomes aware.

hh.06-SE.02
Once the enrolling Authorized User provides a Registered User with training to familiarize them with the Exchange, the enrolling Network will assign him or her a unique identifier and

password that contains at least 7 digits including at least 2 alpha digits and 2 numeric digits. Authorized Users must change their passwords at least every 180 days and may not re-use a password. Passwords shall be case sensitive.

ph.06-SE.02
Hospital shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on Hospital's computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from Hospital's facility using the Exchange. Hospital shall report to the relevant Data Provider any use or disclosure of Data created at that Data Provider of which Hospital becomes aware that is not permitted or required by this Agreement or by law.

SE.03 Administrative Safeguards

mm.06-SE.03
Upon request, each Network member hospital will follow its internal policies and procedures for providing an accounting of disclosures to the patient or patient's representative requesting the accounting, in order to indicate who has accessed the patient's information for treatment provided at that member hospital's system.

mm.06-SE.03
Each Network member hospital will be responsible for initiating, updating, monitoring, controlling, and removing or suspending access of its Authorized Users in Exchange.

sp.08-SE.03
Maintain such policies, procedures and systems as may be necessary to prevent Unauthorized parties from having Access to, Using, Disclosing, Processing, Copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the availability, accessibility, integrity, structure, format or content of information which may be Transmitted to the Receiving Party.[18]

hh.06-SE.03
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

hh.06-SE.03
5.3 Audit Trails.

a. Each Network will record each time an Authorized User accesses the Exchange and will record every item of patient information accessed by the Authorized User.

b. The audit trail will identify whether the Authorized User "overrode" the system to access information of patients with whom the user does not have a pre-existing relationship.

c. Each Network will review the audit trails of information accessed to identify and investigate any potential abuses or violations of the Exchange Policies and Procedures or applicable federal or state laws or regulations.

d. Upon request, each Network will follow its internal policies and procedures for providing an accounting of disclosures to the patient or patient's representative requesting

[18] Such controls are required for electronic Transmissions over a network under the Draft Security Rule at 43, 268, 45 CFR sec. 142.308(d).

the accounting, in order to indicate who has accessed the patient's information for treatment provided.

sp.02-SE.03
(xii) Safeguard means an action, policy, procedure, device, process, technique or other measure intended to prevent the use or disclosure of Protected Information other than as provided for in this Agreement, or to reduce an information system's vulnerability to unauthorized access or use.

mm.06-SE.03
Procedures shall be in place to ensure that purged PHI cannot be misused or placed into active operation in [State Organization] without appropriate authorization.

hh.06-SE.03
Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party

hh.06-SE.03
Access by Authorized Users, Registered Users, Contractors and Staff. Each Network shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data.

ph.06-SE.03
1. Patient Access. [State Organization] hereby authorizes Patient to have access only to their own information contained in the Network and the Databases, for the following uses and purposes:

- Patient's own healthcare treatment.
- Payment of Patient's healthcare services.
- Auditing and monitoring compliance with the terms and conditions of this Agreement.

pp.05-SE.03
In order to protect the security and integrity of the health information provided by and through [Entity], [Entity] requires each individual health care provider who is authorized to have access to such information to enter into an Individual Provider Information Sharing Agreement in the form attached as Appendix A, including an agreement to follow the [Entity]'s User's Manual and appendices describing the Information Services and [Entity]'s Fee Schedule, as these may be updated from time to time. The terms and conditions of the Provider Agreement, the User's Manual, the Information Services and the Fee Schedule, as they exist and as they may be updated from time to time, are therefore incorporated in this Entity Agreement by reference.

pp.05-SE.03
[Entity] shall implement an internal Privacy Compliance Plan, including at least (a) an information technology system which supports database privacy and system security including user authentication, data encryption, and monitoring and keeping a record of all database access, storage and data retrieval transactions by system users, (b) the establishment and maintenance of standards and procedures to be followed by [Entity] employees for the protection of privacy, (c) hiring policies designed to prevent persons with a propensity to invade the privacy of others from having access to information, (d)

monitoring and other procedures intended to detect and prevent unauthorized access to information, and (e) disciplinary procedures for [Entity] employees who breach such standards and procedures.

ph.06-SE.03
Provider agrees to regularly monitor and audit access to [State Organization] and report any issues to [State Organization] upon discovery. Provider shall immediately notify [State Organization] of the revocation of an individual's access and will provide a follow-up report regarding the breach/violation within sixty (60) days of such breach/violation.

ph.02-SE.03
Administrative, physical and technical safeguards which are reasonable and appropriate for the protection of the confidentiality of data subject to this Agreement.

pp.06-SE.03
Section 8.02 Safeguards. Business Associate agrees to use reasonable and appropriate administrative, physical and technological safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. In addition, by April 21, 2005 (or such other later compliance date as established by the United States Secretary of Health and Human Services), Business Associate shall implement such safeguards and security measures as are necessary to comply with the HIPAA Security Standards as set forth in 45 CFR Parts 160, 162, and 164. Business Associate shall provide periodic reports to the Management Committee related to the security measures implemented by Business Associate for the Network, including any security issues that have arisen since any prior report. The provisions of this Section with regard to the security of records management shall survive the termination of this Agreement.

pp.05-SE.03
[Entity] shall implement an internal Privacy Compliance Plan, including at least (a) an information technology system which supports database privacy and system security including user authentication, data encryption, and monitoring and keeping a record of all database access, storage and data retrieval transactions by system users, (b) the establishment and maintenance of standards and procedures to be followed by [Entity] employees for the protection of privacy, (c) hiring policies designed to prevent persons with a propensity to invade the privacy of others from having access to information, (d) monitoring and other procedures intended to detect and prevent unauthorized access to information, and (e) disciplinary procedures for [Entity] employees who breach such standards and procedures.

pp.05-SE.03
[Entity] shall implement an internal Privacy Compliance Plan, including at least (a) an information technology system which supports database privacy and system security including user authentication, data encryption, and monitoring and keeping a record of all database access, storage and data retrieval transactions by system users, (b) the establishment and maintenance of standards and procedures to be followed by [Entity] employees for the protection of privacy, (c) hiring policies designed to prevent persons with a propensity to invade the privacy of others from having access to information, (d) monitoring and other procedures intended to detect and prevent unauthorized access to information, and (e) disciplinary procedures for [Entity] employees who breach such standards and procedures.

mm.07-SE.03
a. Prior to receiving a passcode or other necessary tools for accessing [State Organization], a person must have both their identity and authority verified in accordance with the procedures described below.

b. The following forms of identification are sufficient for verifying a person's identity:

- Official and valid state ID (driver's license, state ID card);
- Official and valid federal ID (passport, military or government ID); or
- Official and valid entity-issued picture ID.

mm.07-SE.03
c. The following items are sufficient for verifying a person's authorization to access [State Organization]:

- Entity-issued ID indicating authorization to access [State Organization];
- Authorization on official entity letterhead from the Privacy Officer or other person designated to determine access levels for [State Organization]; or
- Email authorization from the official entity email address of the Privacy Officer or other person designated to determine access levels for [State Organization].

mm.07-SE.03
d. If a person provides sufficient documentation to meet the requirements of subsections (b) and (c) above, a passcode or other necessary tools for accessing [State Organization] may be issued. At the time of issuance, the person supplying the passcode or other necessary tools should place a copy of the identification and authorization documents in the designated [State Organization] Verification File.

mm.07-SE.03
e. If a person provides any other type of identification or authorization (student ID, court order, etc.), please contact the Privacy Officer or other person designated by this entity to determine access levels for [State Organization].

mm.07-SE.03
f. The majority of persons requiring access to [State Organization] should have their identification and authorization verified prior to any necessary use of the system. For this reason, emergency access to [State Organization] should not be necessary. If, however, a person requests emergency access, the entity should contact an on call provider with access to the system to assess the totality of the situation on a reasonableness basis.

ph.06-SE.03
[State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network) to have access to his/her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.

- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-SE.03
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:]

sp.02-SE.03
g. The [Program] Management Committee shall maintain an information security Program providing reasonable and appropriate administrative, physical and technical Safeguards for the [Program] Cardiac Registry. The Safeguards implemented shall be reasonably consistent with the standards and specifications of the HIPAA Security Rule, as determined by the [Program] Management Committee in the exercise of reasonable discretion.

sp.02-SE.03
(iv) The Participant will use appropriate safeguards to prevent the use or disclosure of the information for any purpose other than those specified in Subsection 6(b)(i);

sp.02-SE.03
(v) The Participant will report to the [Program] Management Committee any use or disclosure of the information for any purpose other than those specified in Subsection 6(b)(i);

ph.05-SE.03
To use appropriate safeguards to prevent use or disclosure of the information other than as provided for by this Agreement.

hh.06-SE.03
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

hh.06-SE.03
6.2 Each Network shall assure that Authorized Users implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on the Authorized User's computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from the Authorized User's location using the Exchange.

mm.06-SE.03
Audit Trails AO.03/mm.06/(SII(C) – Exchange will record each time an Authorized User accesses the Exchange and will record every item of patient information accessed by the Authorized User. The audit trail will identify whether the Authorized User "overrode" the system to access information of patients with whom the user does not have a pre-existing relationship. Since ED clinicians and ED physicians are not required to have a pre-existing relationship with a patient, their overrides are not recorded in the audit trail.

Each Network member hospital routinely will review the audit trails of information accessed from its facility to identify and investigate any potential abuses or violations of the Exchange Policies and Procedures or applicable federal or state laws or regulations.

sp.08-SE.03
Exchange will establish warnings and automatic e-mail alerts to the Data Provider and to Network when it detects erratic usage or anomalies by an Authorized User or any other user (e.g., an Authorized User overrides the system five times within five minutes).

mm.10-SE.03
Delegation rights

Delegation is often necessary in daily operation. In order to be able to keep this under control delegation rights have to be specified in the Agreement since it is particularly difficult to know who has which rights inside and between the domains**.**

sp.08-SE.03
[Immunization] Registry personnel and their authorized agents will audit activities on the [Immunization] Registry to ensure the ongoing security of the data contained therein. Each employee or agent having access to the [Immunization] Registry will sign an Employee Security and Confidentiality Agreement.

mm.10-SE.03
Validity time

Authorization, roles, attestation rights, delegation rights shall have a well defined and specified time period for the access rights to information both within the domain and across domain borders. These time periods shall be notified in the Agreement.

sp.08-SE.03
Maintain technological systems and procedures to guard against unauthorized access to information that is Transmitted electronically, including encryption and/or appropriate technical security mechanisms;[19]

Maintain such policies, procedures and systems as may be necessary to prevent Unauthorized parties from having Access to, Using, Disclosing, Processing, Copying, modifying, corrupting, rendering unavailable, introducing computer code into or otherwise performing activities or operations upon or harmful to the privacy, availability, accessibility, integrity, structure, format or content of information which may be Transmitted to the Receiving Party;[20]

sp.08-SE.03
Notify the Disclosing Party immediately in the event of any proven or suspected incident in which the Receiving Party has reason to believe any Unauthorized person may have had Access to the computer or computer systems of the Receiving Party; [21]

[19] See Draft Security Regulation at 43,268, 45 CFR sec. 142.308(d); and HCFA Internet Security Policy. Note that the systems used to Receive information must be compatible with Disclosing Party systems used to Transmit to the Receiving Party.

[20] See Draft Security Regulation, 45 CFR sec. 142.308(a) – (c).

[21] This provision is also required to comply with the Business Associate Contract provisions of the Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(B), in the context of computerized transactions.

SE.04 Technical Safeguards

mm.10-SE.04
If this is not possible it shall be specified in the Agreement which security level in one domain corresponds with which security level in another domain and authority for the users has to be designed for the various levels in both domains.

mm.10-SE.04
Authorization

The authorization process shall be defined in the Policy Agreement both internally in the domain and externally in the other jurisdiction domains.

mm.10-SE.04
Authentication of Users/Role

Specify the minimal user and role authentication strength (password rules, 2-factor, certificates, etc)

mm.10-SE.04
User/Role Certificates Management

Specify how user authentication security certificates will be managed for the XDS Affinity Domain. For example, it should state which certificate provider(s) will be allowed and how the certificates can be obtained. It should also specify whether or not user certificates will also incorporate information regarding their role, etc.

mm.10-SE.04
Information Access

How access to the information should be controlled in the XDS Affinity Domain, depending upon whether it is contained on a computer system, removable media, or being transferred over a network.

mm.10-SE.04
Security Audit Log Access

Specify how access to the security audit logs will be managed.

mm.10-SE.04
Network Communication Access Security Requirements

Specify the network access security requirements for the XDS Affinity Domain. Specify the means by which network communication security will be ensured (will all Transactions have to be secured by

mm.10-SE.04
Node Access Security Requirements

Specify the system node access security requirements. For example, whether or not all nodes must conform to the IHE ATNA Secure Node Actor/Profile**.**

mm.10-SE.04
Removable Media Access Security Requirements

Whether or not media transfer of XDS content is permitted as part of the XDS Affinity Domain, and if so what media security is required if any. For example, must the media itself be encrypted, or the individual files?

mm.10-SE.04
Network Communication Integrity Requirements

How will integrity of data transmitted over a (cable or wireless) network within the XDS Affinity Domain be managed? What methods for checking this integrity should be used and whether it is mandatory or not for systems acting as specific Actor/Profiles.

mm.10-SE.04
Note that security related configuration should be defined in the appropriate sub-sections of X.11 Technical Security.

hh.06-SE.04
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

hh.06-SE.04
6.2 Each Network shall assure that Authorized Users implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on the Authorized User’s computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from the Authorized User’s location using the Exchange

hh.06-SE.04
c. Each Network will establish warnings and automatic e-mail alerts to the Authorized User and to the other Network when it detects erratic usage or anomalies by an Authorized User or any other user (e.g., a Registered User overrides the system five times within five minutes).

hh.06-SE.04
c. Each Network will establish warnings and automatic e-mail alerts to the Authorized User and to the other Network when it detects erratic usage or anomalies by an Authorized User or any other user (e.g., a Registered User overrides the system five times within five minutes).

sp.02-SE.04
The [Program] Management Committee shall maintain an information security Program providing reasonable and appropriate administrative, physical and technical Safeguards for the [Program] Cardiac Registry. The Safeguards implemented shall be reasonably consistent with the standards and specifications of the HIPAA Security Rule, as determined by the [Program] Management Committee in the exercise of reasonable discretion.

hh.06-SE.04
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

hh.06-SE.04
c. Each Network will establish warnings and automatic e-mail alerts to the Authorized User and to the other Network when it detects erratic usage or anomalies by an Authorized

User or any other user (e.g., a Registered User overrides the system five times within five minutes).

hh.06-SE.04
3.1 Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party.

hh.06-SE.04
3.1 Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party

mm.06-SE.04
Internet connectivity or remote access tied directly to [State Organization] must be secure.

ph.06-SE.04
10.4 Malicious Software, Viruses, and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO's System. The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including without limitation the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine, or data (including without limitation malicious software or "malware," viruses, worms, and Trojan Horses) which will disrupt the proper operation of the System or any part thereof or any hardware or software used by [SNO Name] in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by [SNO Name] or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

ph.06-SE.04
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:]

pp.05-SE.04
The Provider shall ensure that each individual system user's personal authentication identity and password is disclosed only to persons authorized by the Provider to assist in procuring health care information about patients, and that such user(s)' identity and password is supplied to [Entity] prior to such person having access to the [Entity] system on behalf of the Provider. In the event the Provider discovers that the password is known to an unauthorized person, the Provider shall notify [Entity] at once. [Entity] shall cancel any such disclosed password, and require the Provider to establish a new password for such user.

ph.02-SE.04
Administrative, physical and technical safeguards which are reasonable and appropriate for the protection of the confidentiality of data subject to this Agreement.

mm.10-SE.04
The signatories agree that it would be impractical to attempt to adopt uniform standards for the protection of health data at this time or to attempt to impose law related to the privacy of health data of one signatory on another. The signatories therefore agree to transmit health data subject to the understanding that it will be maintained and kept by receiving signatories according to the laws or regulations by which the receiving signatories are bound. Nothing in this Annex shall be construed so as to require any signatory to transmit health data in contravention of the laws or regulations under which the sending signatory is bound. The signatories will comply with the [Labs] MOU where applicable to the exchange of health data.

pp.06-SE.04
Section 8.02 Safeguards. Business Associate agrees to use reasonable and appropriate administrative, physical and technological safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. In addition, by April 21, 2005 (or such other later compliance date as established by the United States Secretary of Health and Human Services), Business Associate shall implement such safeguards and security measures as are necessary to comply with the HIPAA Security Standards as set forth in 45 CFR Parts 160, 162, and 164. Business Associate shall provide periodic reports to the Management Committee related to the security measures implemented by Business Associate for the Network, including any security issues that have arisen since any prior report. The provisions of this Section with regard to the security of records management shall survive the termination of this Agreement.

mm.04-SE.04
Certification Authority: Certifies that (a) Digital Signatures Come from the Correct Party and/or (b) Contents of Electronic Documents are Unchanged.

Subscribers to Certification Authority Generate "Private Keys" and "Public Keys."

"Key:" Digital Code Sequence Subject to Mathematical Transformation.

mm.04-SE.04
Hashing = Mathematical Transformation of Electronic Document Into Unique "Hash Result."
NOTE: Hashing is Applied to Digital Signatures Too.

mm.04-SE.04
Firewalls: Screen and limit access from external sources into internal network.

Encryption: Converts legible information into code readable only by application of key which is retained by sender and receiver.

Authentication: Devices, including passwords and digital signatures, to ensure identity of authorized users.

pp.05-SE.04
The Insurer shall ensure that each individual system user's personal authentication identity and password is disclosed only to individuals authorized by the Insurer to assist in procuring Immunization Data about Enrollees, and that such user(s)' identity and password is supplied to [Entity] prior to such individual having access to the [Entity] system on behalf of the

Insurer. In the event the Insurer discovers that the password is known to an unauthorized individual, the Insurer shall notify [Entity] at once. [Entity] shall cancel any such disclosed password, and require the Insurer to establish a new password for such user.

pp.05-SE.04
The Provider shall ensure that each individual system user's personal authentication identity and password is disclosed only to individuals authorized by the Provider to assist in procuring health care information about patients, and that such user(s)' identity and password is supplied to [Entity] prior to such individual having access to the [Entity] system on behalf of the Provider. In the event the Provider discovers that the password is known to an unauthorized individual, the Provider shall notify [Entity] at once. [Entity] shall cancel any such disclosed password, and require the Provider to establish a new password for such user.

ph.06-SE.04
Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to Authorized Users. Based on the information provided by the Participant pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

mm.09-SE.04
Describe the mechanism(s) for sharing the data such as whether the dataset will be a separate copy of data exposed to shared use outside of the institutions security firewall or the data will be accessed through the firewall.

mm.09-SE.04
Describe what controls the institution expects to place on access to the data, if any and how authorized access will be administered (e.g., will there be a requirement for registration of individual users who must sign (electronically or physically) a data use agreement, either a standard click-through agreement presented by [Network] or a separately negotiated agreement between each prospective user and the research institution?)

SE.05 Physical Safeguards

hh.06-SE.05
6.2 Each Network shall assure that Authorized Users implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on the Authorized User’s computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from the Authorized User’s location using the Exchange

hh.06-SE.05
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

hh.06-SE.05
3.1 Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party

sp.02-SE.05
The [Program] Management Committee shall maintain an information security Program providing reasonable and appropriate administrative, physical and technical Safeguards for the [Program] Cardiac Registry. The Safeguards implemented shall be reasonably consistent with the standards and specifications of the HIPAA Security Rule, as determined by the [Program] Management Committee in the exercise of reasonable discretion.

ph.06-SE.05
10.2 System Security. The Participant's obligations to implement reasonable and appropriate measures to maintain the security of the SNO System and to notify the SNO of breaches in security. The Participant shall implement security measures with respect to the System and the Services in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also adopt and implement the additional security measures described below:]

hh.06-SE.05
b. Each Network shall put into place (and assure that each Authorized User puts into place) protections against unauthorized access.

ph.06-SE.05
10.4 Malicious Software, Viruses, and Other Threats. Requirements that Participants take appropriate measures to prevent damage to the SNO's System. The Participant shall use reasonable efforts to ensure that its connection to and use of the System, including without limitation the medium containing any data or other information provided to the System, does not include, and that any method of transmitting such data will not introduce, any program, routine, subroutine, or data (including without limitation malicious software or "malware," viruses, worms, and Trojan Horses) which will disrupt the proper operation of the System or any part thereof or any hardware or software used by [SNO Name] in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action will cause the System or any part thereof or any hardware, software or data used by [SNO Name] or any other Participant in connection therewith, to be destroyed, damaged, or rendered inoperable.

mm.06-SE.05
Exchange will establish warnings and automatic e-mail alerts to the Data Provider and to Network when it detects erratic usage or anomalies by an Authorized User or any other user (e.g., an Authorized User overrides the system five times within five minutes).

ph.06-SE.05
5.3 Passwords and Other Security Mechanisms. How security mechanisms will be administered, including without limitation how log-on passwords will be provided to

Authorized Users. Based on the information provided by the Participant pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall issue a user name and password [and/or other security measure] to each Authorized User that shall permit the Authorized User to access the System and use the Services. [SNO Name] shall provide each such user name and password [and/or other security measure] to the Participant and the Participant shall be responsible to communicate that information to the appropriate Authorized User. When the Participant removes an individual from its list of Authorized Users, and informs [SNO Name] of the change, pursuant to Section 5.1 (Identification of Authorized Users), [SNO Name] shall cancel the user name and password [and/or other security measure] of such individual with respect to the Participant, and cancel and de-activate the user name and password [and/or other security measure] of such individual if that individual is as a result of the change no longer an Authorized User of any Participant.

hh.06-SE.05
Security and Confidentiality. Each Network shall be responsible for ensuring the security and confidentiality of the Data within its Exchange to which the Authorized Users are granted access, including, without limitation, all user IDs and passwords assigned to Authorized Users and Registered Users. Each Network shall assure that Authorized Users shall not disclose their Data User Accounts to any third party

mm.06-SE.05
Provider personnel must restrict access to [State Organization] workstations to personnel who have a legitimate and identified need to have such access, and who have been granted such access in accordance with the [State Organization] Identification and Authorization Verification Policy and Procedure.

ph.02-SE.05
Administrative, physical and technical safeguards which are reasonable and appropriate for the protection of the confidentiality of data subject to this Agreement.

pp.06-SE.05
Section 8.02 Safeguards. Business Associate agrees to use reasonable and appropriate administrative, physical and technological safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. In addition, by April 21, 2005 (or such other later compliance date as established by the United States Secretary of Health and Human Services), Business Associate shall implement such safeguards and security measures as are necessary to comply with the HIPAA Security Standards as set forth in 45 CFR Parts 160, 162, and 164. Business Associate shall provide periodic reports to the Management Committee related to the security measures implemented by Business Associate for the Network, including any security issues that have arisen since any prior report. The provisions of this Section with regard to the security of records management shall survive the termination of this Agreement.

SP.06-SE.05
The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (http://www.whitehouse.gov/omb/circulars/a130/a130.html), which sets forth guidelines for security plans for automated information systems in Federal agencies. The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the file(s) specified in

section 7 is prohibited. Further, the User agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 4 without written approval from CMS.

mm.09-SE.05
Describe any mechanisms in place within the institution (that is, mechanisms, if any, other than the authentication and authorization controls available either in the application itself or via the [Network] Common Security Module) that will be used for limiting access to authorized users. Note any differences where different types of data sets (as described above) may be involved.

mm.06-SE.05
Once the enrolling hospital provides an Authorized User with training to familiarize them with Exchange, the enrolling hospital will assign him or her a: (i) User ID that contains the abbreviation of the hospital (see below), the user's first initial, and the user's last name (e.g., RHJ Jones); and (ii) password that contains at least 7 digits including at least 2 alpha digits and 2 numeric digits. Authorized Users must change their passwords at least every 180 days and may not re-use a password. Passwords shall be case sensitive.

mm.06-SE.05
The first time an Authorized User logs into Exchange, he or she will view an Exchange Agreement detailing the permitted uses of the system, HIPAA compliance requirements and the user's roles and responsibilities. The Authorized User must click "I Agree" to continue using Exchange. Each Authorized User's consent to the agreement will be logged in the audit trail. The Authorized User may print a copy of the Agreement from their "preferences" section in Exchange.

The enrolling hospital immediately shall remove an Authorized User's access to the Exchange if the user is no longer employed or otherwise associated with the hospital.

SE.06 Agents/Subcontractors of the Participant

pp.05-SE.06
[Entity] shall provide the Provider with a confidential authentication and password security solution for purposes of accessing [Entity]'s database system. The User's Manual shall specify the procedures for access to the [Entity] database system by the Provider and the Provider's employees, contractors, staff, agents or other affiliated individuals authorized to act on behalf of the Provider under this Agreement, and [Entity] shall provide training in the use of the [Entity] security solution. Once the User's Manual and the [Entity] training have been provided, the Provider shall ensure that the Provider and the Provider's employees, contractors, staff, agents or other affiliated individuals comply with the terms of this Agreement and the User's Manual at all times in using the [Entity] system.

pp.05-SE.06
[Entity] shall provide the Provider with a confidential authentication and pass word security solution for purposes of accessing [Entity]'s database system. The User's Manual shall specify the procedures for access to the [Entity] database system by the Provider and the Provider's staff, and [Entity] shall provide training in the use of the [Entity] security solution. Once the User's Manual and the [Entity] training have been provided, the Provider shall ensure that the Provider and the Provider's staff comply with the terms of this Agreement and the User's Manual at all times in using the [Entity] system.

pp.05-SE.06
[Entity] shall provide the Insurer with a confidential authentication and password security solution for purposes of accessing [Entity]'s database system. The Insurance User's Manual shall specify the procedures for access to the [Entity] database system by the Insurer and the Insurer's employees, contractors, officers or agents authorized to act on behalf of the Insurer under this Agreement, and [Entity] shall provide training in the use of the [Entity] security solution. Once the Insurance User's Manual and the [Entity] training have been provided, the Insurer shall ensure that the Insurer and the Insurer's employees, contractors, officers or agents comply with the terms of this Agreement and the Insurance User's Manual at all times in using the [Entity] system.

ph.06-SE.06
9.4.4. Agents, Subcontractors. [SNO Name] shall ensure that its agents, including any subcontractor, to whom [SNO Name] provides Protected Health Information agree to the restrictions and conditions that apply to [SNO Name] with respect to such information and implement the safeguards required by Section 9.4.2 (Appropriate Safeguards) with respect to electronic Protected Health Information.

sp.08-SE.06
Only personnel whose assigned duties include functions associated with the immunization of children can be given access to Registry information. All personnel including permanent and temporary employees, volunteers, contractors, and consultants will be required to sign a [Immunization] Registry User Security and Confidentiality Agreement before gaining access to the Registry. Whenever a user terminates the employment or other status, that person's [Immunization] Registry user account must be removed immediately. A user taking an extended leave of absence must have the account status set to Inactive. Users who fail to access the [Immunization] Registry for more than 60 consecutive days will have their accounts inactivated by [Immunization] Registry.

mm.10-SE.06
Role Management

Specify the Roles defined for users in the XDS Affinity Domain**.**

mm.10-SE.06
Attestation rights

The Policy Agreement shall name the individuals in the organization who have the right to assign roles and attestation authority to employees. An employee with attestation authority has the right to attest medical information.

SE.07 Miscellaneous Security Provisions

mm.10-SE.07
Node Authentication

Specify what mechanisms of node authentication will be used.

mm.10-SE.07
Node Certificates Management

Specify how node security certificates will be managed for the XDS Affinity Domain. For example, it should state which certificate provider(s) will be allowed and how the certificates can be obtained.

mm.10-SE.07
Document Digital Signature Requirements/Policy

Is it necessary to digitally sign any of the content in order to ensure the lifetime integrity of the data, or to allow authentication of the identity entity that created, authorized, or modified the content.

mm.10-SE.07
Secure audit trail
<Change to only talk about ATNA>
As mentioned above, all transactions shall be logged. In most cases this will be done using the ATNA Profile. The technology used and the extent of the logging, shall be specified. If some legacy systems of the Affinity Domain do not support ATNA then how will these be supported.

mm.10-SE.07
Specify whether or not ATNA Audit Record Repositories will be centralized or distributed. In addition, state whether or not they will be expected to support the following, and if so how:

- Filtering
- Reporting
- Alerting
- Alarming
- Forwarding to other Audit Record Repositories

mm.10-SE.07
Consistent Time

In order to be able to ensure high quality logging, time stamping is necessary. All information transactions shall have a time stamp. Specify how support for the IHE Consistent Time Profile will be implemented, and who will be responsible for providing Consistent Time servers. This may require substantial reprogramming of older system and therefore may not possible for economical reasons. In this case the parties signing the Agreement shall decide what can be done under existing circumstances and what measures shall be taken for improving the situation. An implementation plan is part of the Agreement.

mm.10-SH.06
Audit check

The agreement shall stipulate when, by whom and how the log files shall be checked and appropriate action taken.

mm.10-SE.07
Risk analysis

If risks are observed all parties have jointly to evaluate them and decide whether the risks can be accepted or not. The risks have to be documented in the Policy Agreement. If the risks can be accepted all parties shall approve it. If the risks are not acceptable a plan detailing resource requirements for risk reduction shall be included in the Policy Agreement.

mm.10-SE.07
What will the frequency of risk assessments be? Is recommended that they be done at least on an annual basis.

sp.09-SE.07
Security-related agreements (for both data providers and users)

sp.09-SE.07
The DSSF provides an organization with a conceptual framework and implementing tools that facilitate an organization's data sharing activities. The DSSF implementing tools include a decision support tool that uses four types of factors to assess the sensitivity of any given dataset and to determine the desired data access controls.

sp.09-SE.07
The Center will be expected to participate in the testing and refinement of DSSF by providing information about particular data sets it may share via the [Network] infrastructure and by determining the appropriate levels of data sensitivity and secured access controls for each dataset.

sp.09-SE.07
The Center will contribute actively to the testing of security controls that will be defined over the coming months by reviewing [Program] policy statements and providing expert input on the various levels of data access protections from the institution's perspective.

mm.10-SE.07
The signatories recognize the importance of safeguarding individuals' privacy in exchanging and using health data while simultaneously recognizing a compelling interest on the part of the state and provincial signatories to share health data to prevent, detect and respond to public health emergencies for the protection of public health and safety.

mm.06-SE.07
The Provider will discipline, as appropriate, any person who violates the Provider's security policies and procedures and/or causes the Provider to violate the Provider Participation Agreement with [State Organization].

sp.06-SE.07
The User agrees that the authorized representatives of CMS or DHHS Office of the Inspector General will be granted access to premises where the aforesaid file(s) are kept for the purpose of inspecting security arrangements confirming whether the User is in compliance with the security requirements specified in paragraph 9.

mm.09-SE.07
Describe different expected levels of data access (e.g., public access, group or consortium access, or private access, which is generally limited to the originators of the data and/or individually authorized and authenticated individuals/institutions). (Note that certain federally funded research may be subject to specific data sharing/data access requirements in which case, describe the requirements and how the requirements will be met.)

mm.09-SE.07
Information about the institutional units involved in approval to share data outside of the institution, including an IRB.

Are there internal organizations other than an IRB involved in approving the adoption project and sharing data such as Technology Transfer Offices, Compliance, Privacy or Information Technology Security Offices, Legal Counsel, etc.? If so, describe the steps and approximate timeframes of the process for securing all necessary approvals, including what information the organization may require regarding the project, [Network] security or the [Program] itself.

mm.09-SE.07
If there is an IRB involved in approving data sharing, describe the steps and approximate timeframes involved in the process for securing approval to share the particular data involved in the adoption project, if any, including what information the organization may require regarding the project, [Network] security or the [Program] itself.

mm.09-SE.07
Does the IRB audit compliance with the options participants choose in the informed consent? Provide information about any additional anticipated challenges, limitations, or other constraints on data sharing.

mm.10-SE.07
Technical Security

This section details the technical aspects of security for the XDS Affinity Domain. It is most likely that each domain will have its own security rules. It would be ideal of course if the involved domains can commit themselves to one and the same security model. This is the primary goal and the security standards defined in both CEN and ISO shall be the primary tools to achieve this.

mm.10-SE.07
Refer to the "HIE Security and Privacy through IHE White Paper" for further details on the issues that should be considered when implementing an XDS Affinity Domain.

ph.06-SE.07
Hospital shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the security and integrity of Data on Hospital's computer network, and the confidentiality of all Data displayed, transmitted, or accessed at or from Hospital's facility using the Exchange. Hospital shall report to the relevant Data Provider any use or disclosure of Data created at that Data Provider of which Hospital becomes aware that is not permitted or required by this Agreement or by law.

sp.08-SE.07
Information Protection Obligations of Receiving Parties.

General Obligations. At all times following the Receipt of Protected Information, until such time as the Protected Information is no longer in the Receiving Party's possession or subject to its control.[22]

The Receiving Party shall not Use, Disclose or Process Protected Information for any Purpose not stated in the applicable Specifications Addendum, excepting only as necessary for the proper management and administration or in order to carry out the legal responsibilities of the Receiving Party.[23]

[22] These obligations correspond to general requirements for a Business Associate Contract, see Privacy Rule at 82,808, 45 CFR sec. 164.504(e)2).

[23] See Privacy Rule at 82,808 - 8, 45 CFR sec. 164.504(e)(2)(i)(A), .504(e)(2)(ii)(A) and .504(e)(4)(i).

The Receiving Party shall implement appropriate safeguards to prevent any Use or Disclosure of the Protected Information other than those permitted under this Agreement.[24]

sp.08-SE.07
Maintain such policies, procedures and systems as may be reasonably necessary to ensure the Protection of information against Disclosure, corruption or destruction caused by modification of, harm or damage to computer systems components and storage media pertaining to such information, including but not limited to appropriate backup procedures and contingency plans;[25] and

sp.08-SE.07
Conduct assessments of the policies, procedures and systems used by the Receiving Party to fulfill the obligations of this Section, (i) no less frequently than once each year and (ii) in response to any material breach of security within the scope of this Section.[26]

4.9 Term and Termination (TT)

TT.01 Term

pp.06-TT.01
Section 12.01 Term of the Agreement. The term of this Agreement shall begin on April 14, 2004 and shall last through April 13, 2009. This Agreement shall thereafter automatically renew as of each subsequent April 14 as to each Party unless such Party has provided written notice of its intent to withdraw pursuant to Section 12.03 at least one hundred eighty (180) days before the renewal date. The withdrawal of less than all of the Participants shall not be considered a termination of the Agreement and the remaining Participants shall continue to participate under the terms of the Agreement, as amended.

ph.02-TT.01
a. The term of this Agreement shall begin on the date RESEARCHER receives a counterpart of this Agreement signed by the Data Provider, and shall continue until its termination as provided in this section.

ph.06-TT.01
Term. The term of this Agreement shall begin _____, or upon signature by both parties, whichever is later, and shall continue in force for one year from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ph.06-TT.01
The term of this Agreement shall begin, or upon signature by both parties, whichever is later, and shall continue in force for years from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such

[24] See Privacy Rule at 82,808, 45 CFR sec. 164.504(e)(2)(ii)(B).

[25] A Receiving Party will only be required to comply with the final HIPAA security rule if it is also a Covered Entity. This Agreement does not attempt to specify that such compliance is required, but Covered Entities entering into this Agreement as Disclosing Parties may wish to add such a specification applicable to Receiving Parties which are not Covered Entities.

[26] Such assessments are prudent practice, and also required under the Draft Security Rule at 43,266-267, 45 CFR sec. 142.308

renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ph.09-TT.01
1.4 Change or Termination of Services. The SNO's right to change its services or to cease providing services.

Definitions. The definitions of certain important terms used in the Terms and Conditions. Some of these definitions may not correspond to their use in certain other contexts, and are likely to vary if the SNO's organization, operations, system, services and/or relationships with others are different than those assumed by the Model.

ph.06-TT.01
The term of this Agreement shall begin, or upon signature by both parties, whichever is later, and shall continue in force for years from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ph.06-TT.01
5. Term and Termination

This [Participant] Registration Agreement shall continue in effect until it is terminated, in accordance with the [SNO Name] Terms and Conditions.

hh.06-TT.01
8. Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for ________ years.

mm.10-TT.01
Agreement validity period

The time period for which an access Agreement is valid shall be specified in the Agreement. The Agreement shall also include a clause defining the procedure for termination of the Agreement both at the end of the Agreement period and within the Agreement period. Legitimate reasons for cancellation of the Agreement shall be defined. Economic compensations for extra costs if the Agreement is cancelled between the agreed time periods shall also be defined in the Agreement.

Term: The term of this Agreement begins October 1, 2007, and ends September 30, 2009, unless terminated earlier by either party upon thirty (30) days prior written notice.

ph.06-TT.01
Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for five (5) years. Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination. Upon termination, all licenses granted to Hospital relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, Hospital promptly shall return all Access Provider confidential information to Network.

TT.02 Termination Generally

ph.06-TT.02
5. Term and Termination

This [Participant] Registration Agreement shall continue in effect until it is terminated, in accordance with the [SNO Name] Terms and Conditions.

sp.06-TT.02
The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, CMS will cease releasing data to the User under this Agreement and will notify the User either to return all previously released data files to CMS at the User's expense or destroy such data, using the same procedures stated in the above paragraph of this section. Sections 3, 6, 8, 11, 12, 13, 14, 16, 17, and 18 shall survive termination of this Agreement.

ph.06-TT.02
Term. The term of this Agreement shall begin _____, or upon signature by both parties, whichever is later, and shall continue in force for one year from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

mm.04-TT.02
Mutual Audit and Termination Provisions for Breach

ph.02-TT.02
b. Unless terminated sooner by the Data Provider for material breach as provided below, this Agreement shall terminate on the sooner of (i) the date on which RESEARCHER gives written notice to PROVIDER/REPOSITORY and the Data provider that it has completed the research or (ii) REDACTED. Termination for completion of research shall be effective upon receipt of the notice by PROVIDER/REPOSITORY and the Data Provider.

pp.05-TT.02
1. This Agreement may be modified only by the terms of the Insurance User's Manual, as published and updated by [Entity].

pp.05-TT.02
2. This Agreement may be terminated:

pp.05-TT.02
a. By either party effective as of the end of any calendar quarter, by giving written notice of termination received by the other party on or before thirty days before the end of the quarter.

pp.05-TT.02
2. The Providers whose Individual Provider Information Sharing Agreements are covered by this Agreement are identified in Appendix B. In the event of the termination of such an agreement, [Entity] shall notify the Entity in writing, and the Entity's obligation to pay with respect to such Provider shall cease as provided in the terminated agreement. The Entity may discontinue its obligation to pay for any one or all of the Providers covered by this Agreement by written notice to [Entity] received on or before the date thirty days before the end of any calendar quarter, effective as of the end of that quarter.

G. Termination:

pp.05-TT.02
1. This Agreement may be modified only by (a) the terms of the User's Manual, as published and updated by [Entity], (b) the amendment of the Information Services by [Entity], or (c) the amendment of the Fee Schedule by [Entity].

pp.05-TT.02
1. This Agreement may be modified only by (a) the terms of the User's Manual, as published and updated by [Entity], (b) the amendment of the Information Services by [Entity], or (c) the amendment of the Fee Schedule by [Entity].

ph.06-TT.02
This Registration Agreement shall continue in effect until it is terminated, in accordance with the Terms and Conditions and the Policies and procedures.

ph.06-TT.02
K. Upon termination of this Agreement, [State Organization] shall return or destroy all PHI and will retain no copies of such information. If such return or destruction of PHI is not feasible, [State Organization] agrees that the provisions of this Agreement are extended beyond termination to such PHI, and [State Organization] shall limit all further uses and disclosures to those purposes that make the return or destruction of such PHI infeasible.

ph.06-TT.02
Survival of Obligation. Articles III, VIII and X of this Agreement shall survive the expiration or termination of this Agreement.

ph.06-TT.02
The SNO's right to change its services or to cease providing services.

ph.06-TT.02
Alternative One: SNO may change or terminate in sole discretion.

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon notice to Participants.

ph.06-TT.02
OR Alternative Two: SNO may change or terminate upon minimum period of prior notice.

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon not less than ninety (90) days prior notice to Participants.

ph.06-TT.02
OR Alternative Three: SNO may change or terminate upon approval of Management Committee, i.e., body through which Participants and others influence SNO management and governance (see Section 11.6 (Management Committee)).

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time upon the approval of the Management Committee and upon not less than ninety (90) days prior notice to Participants.

Some SNOs may find that certain Participants (e.g., major hospital systems that the SNO determines are essential to the SNO), or their communities generally, will require that the

SNO agree to provide its services for at least a specified term and/or continue to participate in the NHIN. This provision preserves the SNO's rights to change or terminate its services, except as it agrees otherwise in written Registration Agreements with such Participants, as contemplated by Section 4.2 (Registration by Agreement).

ph.06-TT.02
4.10 Effect of Termination. The consequences of terminating a Registration Agreement. Upon any termination of a Participant's Registration Agreement, that party shall cease to be a Participant and thereupon and thereafter neither that party nor its Authorized Users shall have any rights to use the System or the Services. Certain provisions of the Terms and Conditions shall continue to apply to the former Participant and its Authorized Users following that termination, as described in Section 4.11 (Survival Provisions).

ph.06-TT.02
4.11 Survival of Provisions. The provisions of the Registration Agreement that shall continue to bind the Participant following termination. The following provisions of the Terms and Conditions shall survive any termination of a Participant's Registration Agreement: Section 5.5 (Responsibility for Conduct of Participant and Authorized Users), Section 9 (Protected Health Information), Section 13 (Proprietary Information), Section 14.8 (Limitation on Liability) and Section 15.2.1 (Indemnification).

ph.06-TT.02
9.4.9. Action Upon Termination. Given the role of the System and the NHIN, the destruction or return to the Participant of Protected Health Information following the termination of the Participant's Registration Agreement would be infeasible. Therefore, upon termination of the Participant's Registration Agreement, [SNO Name] shall extend the protections of this Section 9.4 (Business Associate Agreement) to such information, and shall limit further use and disclosure of the information to those purposes that make the return or destruction of the information infeasible.

sp.02-TT.02
a. This Agreement may be terminated:

(i) By either party effective as of the end of any calendar quarter, by giving written notice of termination received by the other party on or before thirty days from the end of such quarter.

hh.06-TT.02
Upon termination, all licenses granted to a Network relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, each Network promptly shall return all confidential information to the other.

ph.06-TT.02
Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for five (5) years. Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination. Upon termination, all licenses granted to Hospital relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, Hospital promptly shall return all Access Provider confidential information to Network.

TT.03 Termination for Cause

pp.05-TT.03

2. The Provider acknowledges that other providers who have contracted with [Entity] will rely upon information provided under this Agreement through [Entity] in making decisions concerning patient care as well. The knowing or reckless provision or verification of false or materially inaccurate or materially incomplete information by the Provider may be grounds for termination of this Agreement at once at [Entity]'s discretion, and may expose the Provider to liability for damages in the event that such erroneous information is a cause of harm to a patient.

pp.06-TT.03

Section 12.03 Withdrawal of a Participant. A Participant may withdraw from this Agreement in connection with any renewal of this Agreement pursuant to Section 12.01. Except as provided in the preceding sentence, a Participant may withdraw from this Agreement prior to any renewal of the Agreement only: (a) upon written agreement between the withdrawing Participant and [Organization]; or (b) for cause. The following shall constitute adequate cause for the withdrawal from this Agreement:

pp.06-TT.03

(a) A significant breach of another Participant’s duties of confidentiality under ARTICLE V of this Agreement with regard to Information stored on the Network by the withdrawing Participant, or a significant breach of [Organization]’s duties under ARTICLE VII or ARTICLE VIII with regard to Information stored on the Network by the withdrawing Participant (provided that the Participant has allowed a reasonable time for [Organization] to cure any such significant breach). Any claim of a significant breach by a Party shall be submitted to the Management Committee which will determine, pursuant to Section 10.02 of this Agreement, whether a claimed breach is significant enough to constitute cause under this Agreement. This determination shall be an advisory opinion and shall not be binding on any party to this Agreement and shall not act as a waiver or determination of any Party’s rights under federal, state or local laws. In a vote to determine whether a breach is significant, the complaining party(ies) and the alleged breaching party(ies) shall not participate.

pp.06-TT.03

Excessive and unexpected expenses incurred by the withdrawing Participant as a result of its participation in this Agreement that exceed $10,000 for any given period of twelve (12) months during the term of this Agreement

pp.06-TT.03

The inability of a withdrawing Participant to access its own Information submitted to the Network due to causes controlled by [Organization]. Such inability shall not constitute cause until a Participant has provided notice to [Organization] or its designee that such Information is inaccessible and after [Organization] is unable to cure such inaccessibility after having been given sixty (60) days to do so after notice is provided.

ph.02-TT.03

c. The Data Provider may terminate this Agreement at any time upon the Data Provider’s determination that PROVIDER/REPOSITORY, RESEARCHER, or any contractor of RESEARCHER, has materially breached this Agreement, by giving written notice of termination to RESEARCHER and PROVIDER/REPOSITORY. Termination for material breach shall be effective upon receipt of the notice by RESEARCHER and PROVIDER/REPOSITORY.

pp.05-TT.03
b. By [Entity] at once at its discretion upon [Entity]'s verification of any material breach by the Insurer of the Obligations to Maintain Patient Privacy, or the Insurer's failure to cooperate in any audit initiated by [Entity] to determine whether such a breach may have occurred; or

pp.05-TT.03
c. By the Insurer in the event that [Entity] materially fails to comply with the terms of an agreement between the parties for the provision of specific Immunization Data entered into under Paragraph C(1).

pp.05-TT.03
The Entity acknowledges that the failure to timely pay in full the amounts due under all the Individual Provider Information Sharing Agreements covered by this Agreement may, at [Entity]'s discretion, be grounds for termination of all such agreements.

pp.05-TT.03
2 This Agreement may be terminated by either party effective as of the end of any calendar quarter, by giving written notice of termination received by the other party on or before thirty days before the end of the quarter; provided that [Entity] may terminate this Agreement at once at its discretion upon [Entity]'s verification of any material breach by the Provider of any provision of the Provider's Obligation to Communicate a True, Accurate and Complete Record or Obligations to Maintain Patient Privacy, or the Provider's failure to cooperate in any audit initiated by [Entity] to determine whether such a breach may have occurred.

pp.05-TT.03
iii) The Provider acknowledges that other providers who have contracted with [Entity] will rely upon the information he or she provides and makes use of through [Entity] in making decisions concerning patient care as well. The knowing provision or verification of false or materially inaccurate or materially incomplete information by the Provider may be grounds for termination of this agreement at once at [Entity]'s discretion, and may expose the Provider to liability for damages in the event that such erroneous information is a cause of harm to a patient.

pp.05-TT.03
2. This Agreement may be terminated by either party effective as of the end of any calendar quarter, by giving written notice of termination received by the other party on or before thirty days before the end of the quarter; provided that [Entity] may terminate this Agreement at once at its discretion upon [Entity]'s verification of any material breach by the Provider of any provision of the Provider's Obligation to Communicate a True, Accurate and Complete Record or Obligations to Maintain Patient Privacy, or the Provider's failure to cooperate in any audit initiated by [Entity] to determine whether such a breach may have occurred.

ph.06-TT.03
Access Fee. Participation in the Network may be subject to an access fee. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating patients will have the option to terminate at that time. [Note for Steering Committee: May want to consider nominal fee from the beginning to make further implementation easier.]

ph.06-TT.03
Termination. [State Organization] also reserves the right, within its sole discretion, to suspend or terminate Patient's access upon reasonable suspicion of a violation of this Agreement, or any action that may jeopardize the privacy and security of the Databases. Patient may appeal such termination in accordance with the appeal procedures established by [State Organization].

ph.06-TT.03
Compliance with Law. [State Organization] shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which [State Organization] reasonably believes: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally-funded healthcare program, including the Medicare and Medicaid programs.

ph.06-TT.03
Provider reserves the right to terminate [State Organization]'s use of the PHI at any time that Provider has reason to believe that [State Organization] has violated any of the conditions set forth in paragraphs A-K of Section III, or has accessed any information not described herein for any purpose.

ph.06-TT.03
B. Provider agrees to be bound by the restrictions and conditions of paragraphs A-K of Section III to the extent Provider has access to PHI of other Providers through [State Organization]. [State Organization] reserves the right to terminate Provider's access to the Network and access to the Databases at any time that [State Organization] has reason to believe that Provider has violated any of the conditions set forth in Section III or has accessed any information that Provider would not otherwise be authorized to receive pursuant to this Agreement.

ph.06-TT.03
Participation in the Network may be subject to an access fee or fees, depending on the size of the organization and number of accessing individuals. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating providers will have the option to terminate at that time.

ph.06-TT.03
Notwithstanding any other provision of this Agreement, either party may immediately terminate this Agreement if the other party has materially violated its responsibilities regarding PHI under this Agreement and has failed to provide satisfactory assurances within ten (10) days of notice of such material violation that the violation has been cured and steps taken to prevent its recurrence.

ph.06-TT.03
[State Organization] also reserves the right, within its sole discretion, to suspend or terminate Provider's access (or access of any individual working at Provider) upon reasonable suspicion of a violation of this Agreement, or violation of policies and procedures that may jeopardize the privacy and security of the Databases.

XI. Effect of Governmental Laws and Regulation

ph.06-TT.03
Each party shall have the right to terminate this Agreement to comply with any legal order, ruling, opinion, procedure, policy, or other guidance issued, or proposed to be issued, by any federal or state agency, or to comply with any provision of law, regulation, or any requirement of accreditation, tax-exemption, federally-funded health care program participation or licensure which: (i) invalidates or is inconsistent with the provisions of this Agreement; (ii) would cause a party to be in violation of the law; or (iii) jeopardizes the good standing status of licensure, accreditation or participation in any federally funded healthcare program, including the Medicare and Medicaid programs.

ph.06-TT.03
OR Alternative Three: SNO may change or terminate upon approval of Management Committee, i.e., body through which Participants and others influence SNO management and governance (see Section 11.6 (Management Committee)).

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time upon the approval of the Management Committee and upon not less than ninety (90) days prior notice to Participants.

Some SNOs may find that certain Participants (e.g., major hospital systems that the SNO determines are essential to the SNO), or their communities generally, will require that the SNO agree to provide its services for at least a specified term and/or continue to participate in the NHIN. This provision preserves the SNO's rights to change or terminate its services, except as it agrees otherwise in written Registration Agreements with such Participants, as contemplated by Section 4.2 (Registration by Agreement).

ph.06-TT.03
If a change to the Terms and Conditions described in Section 4.5 (Changes to Terms and Conditions) affects a material right or obligation of a Participant under that Participant's Registration Agreement, and the Participant objects to that change, that Participant may terminate its Registration Agreement by giving [SNO Name] written notice thereof not more than thirty (30) days following [SNO Name]'s notice of the change. Such termination of the Participant's Registration Agreement shall be effective as of the effective date of the change to which the Participant objects; provided, however, that any change to the Terms and Conditions that [SNO Name] determines is required to comply with any federal, state, or local law or regulation shall take effect as of the effective date [SNO Name] determines is required, and the termination of any Participant's Registration Agreement based on the Participant's objection to the change shall be effective as of [SNO Name]'s receipt of the Participant's notice of termination.

ph.06-TT.03
A Participant may terminate its Registration Agreement upon [SNO Name]'s failure to perform a material responsibility arising out of the Participant's Registration Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that failure.

OR Alternative Five: Participant may terminate for specified cause (may be combined with Alternatives Two or Three and/or Four).

ph.06-TT.03
A Participant may terminate its Registration Agreement upon a Serious Breach of Confidentiality or Security, as described in Section 9.3 (Reporting of Serious Breaches),

when such Serious Breach of Confidentiality or Security continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that breach.

4.8 Participant’s Right to Terminate for Breach of Business Associate Agreement.

A Participant’s right to terminate its Registration Agreement based on the SNO’s failure to perform its obligations.

ph.06-TT.03
Notwithstanding any other provision of this Section 4 (Registration Agreements) to the contrary, if Section 9.4 (Business Associate Agreement) applies to a Participant’s Registration Agreement, the Participant may terminate its Registration Agreement as set forth in Section 9.4.10 (Special Termination).

4.9 [SNO Name]’s Right to Terminate Registration Agreements.

How the SNO may terminate a Participant’s Registration Agreement.

ph.06-TT.03
OR Alternative Four: SNO may terminate for cause (may be combined with Alternatives Two or Three).

[SNO Name] may terminate any Participant’s Registration Agreement upon the Participant’s failure to perform a material responsibility arising out of the Participant’s Registration Agreement, and that failure continues uncured for a period of sixty (60) days after [SNO Name] has given the Participant notice of that failure and requested that the Participant cure that failure.

ph.06-TT.03
9.4.10 Special Termination. Notwithstanding any other provision of the Terms and Conditions to the contrary, the Participant may immediately terminate its Registration Agreement if it determines that [SNO Name] has violated a material term of this Section 9.4 (Business Associate Agreement), and [SNO Name] fails to remedy the violation within thirty (30) days following receipt of written notice thereof.

ph.06-TT.03
Notwithstanding any other provision of this Agreement, either party may immediately terminate this Agreement if the other party has materially violated its responsibilities regarding PHI under this Agreement and has failed to provide satisfactory assurances within ten (10) days of notice of such material violation that the violation has been cured and steps taken to prevent its recurrence.

ph.06-TT.03
[State Organization] also reserves the right, within its sole discretion, to suspend or terminate Provider’s access (or access of any individual working at Provider) upon reasonable suspicion of a violation of this Agreement, or violation of policies and procedures that may jeopardize the privacy and security of the Databases.

ph.06-TT.03
4. Changes to Terms and Conditions

The [SNO Name] Terms and Conditions shall be subject to change from time to time, and all such changes shall be incorporated by reference into this [Participant] Registration

Agreement upon the effective date selected by [SNO Name]. The [Participant] shall be informed of all such changes prior to their effectiveness. If the [Participant] objects to the changes, the [Participant] may terminate this Agreement and, by doing so, cease to be a [Participant], as described in the [SNO Name] Terms and Conditions.

sp.02-TT.03
(vii) Upon receipt of a report of an improper use or disclosure of information under Subsection 6(b)(v), the [Program] Management Committee shall notify the Participant(s) who provided the data which was the subject of the use or disclosure. In the event the [Program] Management Committee knows of a pattern of activity or practice that constitutes a material breach of this Subsection 6(b), which the Participant does not take reasonable steps to cure, the [Program] Management Committee may discontinue providing [Program] information to the Participant and notify HHS.

sp.02-TT.03
a. This Agreement may be terminated

(ii) By the [Program] Management Committee immediately at its discretion in the event of the Participant's failure to cooperate in any audit initiated by the [Program] Management Committee to determine whether such a breach may have occurred.

sp.02-TT.03
a. This Agreement may be terminated

(iii) By the Participant immediately in the event of a material failure to receive requested information required to be provided under Appendix A or B.

sp.02-TT.03
a. This Agreement may be terminated

(iv) By the Participant in the event that [Entity] violates a material term of Section 4 and does not take reasonable steps to cure such violation.

sp.02-TT.03
b. This Agreement shall be deemed automatically terminated effective upon the date of exclusion of either party from participation in any government health care program, including but not limited to Medicare, Medicaid, CHAMPUS or Tricare.

ph.05-TT.03
In the event The Regents becomes aware of any use of the Limited Data Set or any part of it that is not authorized under this Agreement or required by applicable law, The Regents may (i) terminate this Agreement upon notice; (ii) disqualify (in whole or in part) the User and/or any Authorized Parties from receiving protected health information in the future; and/or (iii) report the inappropriate use or disclosure to the Secretary of the Department of Health and Human Services. Further sanctions may apply to the User and/or Authorized Parties under 45 C.F.R. parts 160 and 164.

This Health Information Exchange Agreement ("Agreement") is made effective this ____ day of _______, 200_ ("Effective Date"), by and between, a [type of entity] organized under the laws of the State of ______________ and having its principal place of business at ________________, ("A"); and ______________ , a [type of entity] organized under the laws of the State of ______________ and having its principal place of business at ______________ ("B") (each, a "Network" and together, "Networks").

sp.08-TT.03
All individuals who wish to participate as a user of the [Immunization] Registry must sign and comply with the [Immunization] Registry User Security and Confidentiality Agreement. Any use of the [Immunization] Registry that violates the [Immunization] Registry User Security and Confidentiality Agreement will subject the user to revocation of the user's access privileges and may result in civil or criminal penalties for improper disclosure of health information.

TT.04 Termination Without Cause

pp.06-TT.04
Section 12.03 Withdrawal of a Participant. A Participant may withdraw from this Agreement in connection with any renewal of this Agreement pursuant to Section 12.01. Except as provided in the preceding sentence, a Participant may withdraw from this Agreement prior to any renewal of the Agreement only: (a) upon written agreement between the withdrawing Participant and [Organization]; or (b) for cause. The following shall constitute adequate cause for the withdrawal from this Agreement:

ph.06-TT.04
Term. The term of this Agreement shall begin, or upon signature by both parties, whichever is later, and shall continue in force for one year from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ph.06-TT.04
The term of this Agreement shall begin, or upon signature by both parties, whichever is later, and shall continue in force for years from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ph.06-TT.04
Alternative One: SNO may change or terminate in sole discretion. [SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon notice to Participants.

ph.06-TT.04
OR Alternative Two: SNO may change or terminate upon minimum period of prior notice.

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time in its sole discretion upon not less than ninety (90) days prior notice to Participants.

ph.06-TT.04
OR Alternative Three: SNO may change or terminate upon approval of Management Committee, i.e., body through which Participants and others influence SNO management and governance (see Section 11.6 (Management Committee)).

[SNO Name] may cease to participate in the NHIN, or may change the System and/or the Services, or may cease providing the Services, at any time upon the approval of the Management Committee and upon not less than ninety (90) days prior notice to Participants.

Some SNOs may find that certain Participants (e.g., major hospital systems that the SNO determines are essential to the SNO), or their communities generally, will require that the SNO agree to provide its services for at least a specified term and/or continue to participate in the NHIN. This provision preserves the SNO's rights to change or terminate its services, except as it agrees otherwise in written Registration Agreements with such Participants, as contemplated by Section 4.2 (Registration by Agreement).

ph.06-TT.04
A Participant may terminate its Registration Agreement at any time without cause by giving notice of that termination to [SNO Name].

OR Alternative Two: Participant may terminate without cause with prior written notice.

ph.06-TT.04
A Participant may terminate its Registration Agreement at any time without cause by giving not less than _______ days prior notice to [SNO Name].

OR Alternative Three: Participant may terminate as of the next anniversary of having entered into the Registration Agreement.

ph.06-TT.04
A Participant may terminate its Registration Agreement at any time without cause effective as of the next anniversary of the effective date of the Participant's Registration Agreement, by giving not less than _____ days prior notice to [SNO Name].

OR Alternative Four: Participant may terminate for cause (may be combined with Alternatives Two or Three and/or Five).

ph.06-TT.04
Alternative One: SNO may terminate at any time without cause.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant's Registration Agreement without cause by giving notice of that termination to the Participant.

ph.06-TT.04
OR Alternative Two: SNO may terminate without cause with prior written notice.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant's Registration Agreement at any time without cause by giving not less than _______ days prior notice to the Participant.

ph.06-TT.04
OR Alternative Three: SNO may terminate as of the next anniversary of having entered into the Registration Agreement.

Except as provided otherwise in a written Registration Agreement entered into pursuant to Section 4.2 (Registration by Agreement), [SNO Name] may terminate any Participant's Registration Agreement at any time without cause effective as of the next anniversary of the effective date of the Participant's Registration Agreement, by giving not less than _____ days prior notice to the Participant

ph.06-TT.04
The term of this Agreement shall begin, or upon signature by both parties, whichever is later, and shall continue in force for years from such date. Thereafter, the Agreement will automatically renew for additional one (1) year periods, provided that during any such renewal period either party may terminate this Agreement without cause upon giving thirty (30) days prior written notice to the other.

ss.05-TT.04
Signatories are free to withdraw from this Agreement;

ss.05-TT.04
Withdrawal of any signatory from this Agreement is effective 30 days after written notice of intent to withdraw is sent to the other signatories.

hh.06-TT.04
Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination.

ph.06-TT.04
Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for five (5) years. Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination. Upon termination, all licenses granted to Hospital relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, Hospital promptly shall return all Access Provider confidential information to Network.

4.10 Fees/Consideration (FC)

FC.01 Fee Schedule

pp.05-FC.01
F. Billing Information:

1. The Provider will pay [Entity] fees in accordance with the Fee Schedule attached as Appendix B.

pp.05-FC.01
The provider is responsible for payments to [Entity] for use of the [Name] Profile system in accord with the following payment schedule and billing and payment procedures for the information services described in Appendix A.

pp.05-FC.01
$524 per year for each child under the provider’s care for use of all online system features while less than 50% of children under the age of six in the county of the provider’s place of business have immunization records in the [Name] Profile database.

pp.05-FC.01
$1.04 per year for each child under the provider’s care for use of all online system features while less than 75% of children under the age of six in the county of the provider’s place of business have immunization records in the [Name] Profile database.

pp.05-FC.01
$1.56 per year for each child under the provider’s care for use of all online system features when 75% or more of all children under the age of six in the county of the provider’s place of business have immunization records in the [Name] Profile database.

pp.05-FC.01
1. The Provider will pay [Entity] fees in accordance with the Fee Schedule attached as Appendix B.

pp.05-FC.01
The provider is responsible for payments to [Entity] for use of the [Name] Profile system in accord with the following payment schedule and billing and payment procedures for the information services described in Appendix A.

pp.05-FC.01
$524 per year for each child under the provider’s care for use of all online system features while less than 50% of children under the age of six in the county of the provider’s place of business have immunization records in the [Name] Profile database.

pp.05-FC.01
$1.04 per year for each child under the provider’s care for use of all online system features while less than 75% of children under the age of six in the county of the provider’s place of business have immunization records in the [Name] Profile database.

pp.05-FC.01
$1.56 per year for each child under the provider’s care for use of all online system features when 75% or more of all children under the age of six in the county of the providers place of business have immunization records in the [Name] Profile database.

ph.06-FC.01
12.1 Agreed-Upon Fees. Provision for a Participant’s written agreement to take precedence over the SNO Terms and Conditions. If the Participant has entered into a written Registration Agreement with [SNO Name] pursuant to Section 4.2 (Registration by Agreement), the terms and conditions of that Registration Agreement with respect to the payment of fees and charges shall apply.

ph.06-FC.01
12.2 Service Fees.

Alternative One: SNO’s fee schedule is not a part of the SNO Terms and Conditions. Unless the Participant’s Registration Agreement provides otherwise, each Participant shall pay to [SNO Name] [SNO Name]’s Service Fees, in accordance with [SNO Name]’s then-current Fee Schedule, for those Services for which the Participant has registered.

ph.06-FC.01
OR Alternative Two: SNO’s fee schedule is a part of the SNO Terms and Conditions. Unless the Participant’s Registration Agreement provides otherwise, each Participant shall pay to [SNO Name] [SNO Name]’s Service Fees, in accordance with the Fee Schedule attached as Schedule 12.2 (Service Fees), for those Services for which the Participant has registered.

ph.06-FC.01
A SNO’s Fee Schedule may include a variety of fee levels, permitting the SNO to charge greater and lesser amounts to Participants, depending upon the extent to which each elects

to receive Services and/or hardware and software. In addition, the Fee Schedule should address the extent, if any, to which Data Providers are to pay.

sp.02-FC.01
7. Billing Information.

The Participant will pay the [Program] Cardiac Registry usage fees in accordance with the Schedule of Fees attached as Appendix B. The [Program] Management Committee may amend the Schedule of Fees from time to time. Any such change shall be communicated to the Participant in writing, and shall be considered effective and accepted by the Participant as of the beginning of the next calendar quarter which is sixty or more days from the date on which notice is given unless the Participant terminates this Agreement under Subsection

sp.02-FC.01
Appendix B

[Program] FEE SCHEDULE

[Program] BASIC SERVICE PACKAGE

Customer support

Secure and confidential data storage

Advanced statistical analyses, including risk adjustment

Standard institutional and comparative outcomes reporting

The [Program] Basic Service Package includes products and services designed to assist participating providers in data management and reporting relating to a specific category of clinical activities.

Fees for the Basic Service Package include an initial annual payment plus quarterly per case charges based on the number of actual cases submitted to [Program].

Category C-1.0 – CABG and PCI

Annual Fee: Total CABG and PCI cases per year, based on previous four quarters:

< 100 cases $ 2,500
100+ cases $ 3,500
Per Case Fee: $ 17.50

[Program] FEE-FOR-SERVICE OPTIONS

Custom institutional and physician outcomes reporting—charges per request*
Data collection assistance—charges per request*
Authorized data access—charges per request*
Performance improvement consultation—charges per request*
ORYX data submission to JCAHO—charges to be determined*

*[Program] will provide fee-for-service options for participants requesting special products and services. Charges will be determined by [Program] on a per customer basis, depending on the specific requirements of the request.

Custom Institutional and Physician Outcomes Reporting

Customized reporting for institutions and individual physicians may be performed, as authorized by the requesting customer and any providers named in the report. As part of this service, authorized participants and their associated providers may instruct [Program] to provide such reports to third parties, e.g., to satisfy JCAHO or NCQA requirements.

Customized comparative reporting will also be offered for health systems, networks or health care alliances as directed. Proper written authorization will be obtained from all participants and their associated providers that are included in any comparative report.

Data Collection Assistance

A Core Data Set of clinical measures has been defined for collection by [Program] participants and their associated providers. Functional measures that enable longitudinal outcomes assessment will be added. Standard data collection methods include a fax based system described in detail in the [Program] Health Care Provider Procedure Manual. Custom electronic interfaces for batch transmission may be developed by participating providers at their expense.

Beyond facilitation of an operational fax-based system for participants and their associated providers, [Program] will provide on-site data collection assistance, for a nominal fee, as requested by participants.

Authorized Data Access

Participants and their associated providers will be granted authorized access to electronic copies of the raw data they have submitted as provided for in the [Program] Health Care Provider Information Sharing Agreement (see Appendix B). Due to the labor and technology involved in processing such requests, authorized access to raw data will be billed on a customer-by-customer basis.

Performance Improvement Consultation

For a nominal fee, [Program] will provide performance improvement consulting services related to the interpretation and use of standard and custom reports on institutional and cross-institutional performance. [Program] will submit a proposal including professional fees and expenses based on each customer’s specific request for consulting support.

ORYX Data Submission to JCAHO

[Program] will assist providers in their efforts to satisfy accreditation requirements of the Joint Commission on Accreditation of Healthcare Organizations. At the request of participating providers, [Program] will submit data to JCAHO for selected ORYX performance indicators. Pricing for ORYX services will be determined per clinical domain, e.g., cardiac services, obstetric services, asthma or diabetes. Written agreements describing the provision of ORYX services to [Program] customers require yearly renewal.

This data use agreement (the “Agreement”) is by and between The Regents of the University of [State] (“The Regents”), a [State] constitutional corporation with its principal place of business in [City], [State], on behalf of the University of [State] Health System, and ___, a ___ with its principal place of business in ___ (“User”) and is effective as of ___ (the “Effective Date”).

FC.02 Payment of Fees

mm.10-FC.02
Costs and expenses

This Annex does not represent a service contract between the signatories. Equipment and supplies used or expended on behalf and/or at the request of a signatory shall be replaced in kind by that signatory unless the signatories involved reach a different understanding. Similarly, if a signatory incurs costs or expenses in the housing and care of evacuees and/or refugees, the sending signatory shall reimburse the receiving signatory at a rate and in a manner to be determined by the signatories. Reimbursement shall not be in excess of the greater of the actual expenditure made or, in the case of consumables, the replacement cost of the goods consumed.

pp.05-FC.02
A. Assumption of Payment Obligation

1. The Entity hereby agrees to pay the sums due [Entity] under the Individual Provider Information Sharing Agreements entered into by its Providers, in the amounts and under the terms of those Agreements, as billed by [Entity].

pp.05-FC.02
Billing Information:

The Insurer will pay [Entity] fees in accordance with the agreement of the parties.

pp.05-FC.02
Billing and Payment Procedures

1. The Provider will pay [Entity] the above applicable fee on a pro-rata bases each quarter for each Immunization Patient in its care. Within thirty days from the end of each quarter, beginning on the last day of the quarter including the effective date stated below, [Entity] shall send the Provider an invoice listing all Immunization Patients for which such fee is due, including a statement of the total sum due for that quarter. Payment shall be due on or before thirty days from the date of the invoice.

pp.05-FC.02
Billing and Payment Procedures

1. The Provider will pay [Entity] the above applicable fee on a pro-rata bases each quarter for each Immunization Patient in its care. Within thirty days from the end of each quarter, beginning on the last day of the quarter including the effective date stated below, [Entity] shall send the Provider an invoice listing all Immunization Patients for which such fee is due, including a statement of the total sum due for that quarter. Payment shall be due on or before thirty days from the date of the invoice.

ph.06-FC.02
Participation in the Network may be subject to an access fee or fees, depending on the size of the organization and number of accessing individuals. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating providers will have the option to terminate at that time.

ph.06-FC.02
12.1 Agreed-Upon Fees. Provision for a Participant's written agreement to take precedence over the SNO Terms and Conditions. If the Participant has entered into a written Registration Agreement with [SNO Name] pursuant to Section 4.2 (Registration by Agreement), the terms and conditions of that Registration Agreement with respect to the payment of fees and charges shall apply.

ph.06-FC.02
12.5 Payment. The Participant shall pay all Service Fees and any Miscellaneous Charges within thirty (30) days following the date of invoice by [SNO Name] sent to the Participant's address as shown in [SNO Name]'s records or e-mailed in accordance with the Participant's Registration Agreement.

mm.10-FC.02
Organizational Roles

Explain the general economic considerations associated with the implementation of this XDS Affinity Domain shall be provided. These considerations include, but are not limited to:

Funding for system implementation (examples: central private/public source, taxes, documentation of general funding guidelines rather than explicit statement on funding source)

Business model (payments from users, re-imbursement policy, role of insurance, etc.)

ph.06-FC.02
Access Fee. Participation in the Network may be subject to an access fee. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating patients will have the option to terminate at that time. [Note for Steering Committee: May want to consider nominal fee from the beginning to make further implementation easier.]

sp.04-FC.02
Fiscal plan for system operation and maintenance

B. [Program] agrees to:

Pay Participating Clinic, through [Entity] (the payment intermediary for [Program]), as described in Sections A2 to A5 above, for authorized services provided to participants.

Pay its Section B costs or expenses using grant funds received from the United States Department of Health and Human Services. Participating Clinic understands that [Program] is funded by federal grants and state matching funds, and that this Participating Clinic Agreement depends upon the continued availability of appropriated funds and expenditure authority from Congress, the Legislature, or the Executive Branch, for this purpose. If for any reason Congress or the Legislature fails to appropriate funds or grant expenditure authority, or the grant funds or appropriated funds become unavailable by operation of law or federal funds reductions, [Program] will not be liable or responsible to pay any cost or expense or provide services set forth in this Agreement. [Program]'s failure to pay or provide services for any of these reasons is not a default by [Program] nor does it give rise to a claim against [Program] or the State of [State].

ph.06-FC.02
4. Resources for Collaborative Investigations—Funding needed for the travel of investigation participants will be the responsibility of their home public health agency. Primary resources needed for the investigation itself will be the responsibility of the lead public health agency where the investigation takes place. In the absence of needed supplies or investigative capacity (e.g., select laboratory exams), sharing of resources between counterpart agencies is strongly encouraged.

Operational Costs. To support the ongoing costs of Exchange, including the Access Provider maintenance fees and the Host hosting fees, Hospital agrees to pay Network a monthly fee of ___________________and No/100 Dollars ($___________), payable on the first day of each month beginning ______________.

Health care personnel compensation and benefits.

FC.03 Change in Fees

mm.10-FC.03
A sending signatory shall provide, in accordance with its own law, the employment, accident, health and death benefits to health care personnel providing services pursuant to this Annex in a receiving signatory to which they would be entitled for the performance of these services in the sending signatory. Signatories may agree upon a formula for reimbursement of expenses incurred in maintaining these benefits for health care personnel while engaged in service pursuant to this Annex outside the sending signatory.

pp.05-FC.03
2. [Entity] may amend the Fee Schedule from time to time. Any such change shall be communicated in writing to the Provider, and shall be considered in force and accepted by the Provider thirty days from the date the Provider receives written notice of the change, unless [Entity] receives a written objection from the Provider before the end of that thirty day period.

ph.06-FC.03
Access Fee. Participation in the Network may be subject to an access fee. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating patients will have the option to terminate at that time. [Note for Steering Committee: May want to consider nominal fee from the beginning to make further implementation easier.]

ph.06-FC.03
Participation in the Network may be subject to an access fee or fees, depending on the size of the organization and number of accessing individuals. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating providers will have the option to terminate at that time.

FC.04 Additional Costs/Charges

ph.06-FC.04
12.4 Miscellaneous Charges. Unless the Participant’s Registration Agreement provides otherwise, the Participant also shall pay [SNO Name]’s charges for all goods or services that [SNO Name] provides at the Participant’s request that are not specified in [SNO Name]’s then-current Fee Schedule

ph.06-FC.04
12.6 Late Charges. Provision calling for late charges on delinquent Service Fees and Miscellaneous Charges. Service Fees and Miscellaneous Charges not paid to [SNO Name] within ____________ (__) business days following the due date therefore are subject to a late charge of five percent (5%) of the amount owing and interest thereafter at the rate of one and one-half percent (1 _%) per month on the outstanding balance, or the highest amount permitted by law, whichever is lower.

(“Miscellaneous Charges”).

ph.06-FC.04
The Model assumes that the SNO will wish to have strict terms regarding payment by Participants. A SNO may wish to adopt measures that are either more or less strict than shown here.

12.8 Taxes. All Service Fees and Miscellaneous Charges shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future, and the Participant shall pay any tax (excluding taxes on [SNO Name]’s net income) that [SNO Name] may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services provided pursuant to the Terms and Conditions.

ph.06-FC.04
12.9 Other Charges and Expenses.

The Participant shall be solely responsible for any other charges or expenses the Participant may incur to access the System and use the Services, including without limitation, telephone and equipment charges, and fees charged by third-party vendors of products and services.

mm.09-FC.04
1. Preparing for Binational Outbreaks—Pre-event preparations that should be made include:

- Exchange of lists of binational contacts at the local, state, and federal levels
- Contact information which provide for round-the-clock availability
- Mechanisms for communication in both Spanish and English
- Communications protocols for notification of public health officials and planning of needed responses

FC.05 Suspension of Services

ph.06-FC.05
Access Fee. Participation in the Network may be subject to an access fee. [State Organization] will distribute any proposed fee schedule at least thirty (30) days prior to instituting such fee, and participating patients will have the option to terminate at that time. [Note for Steering Committee: May want to consider nominal fee from the beginning to make further implementation easier.]

ph.06-FC.05
12.7 Suspension of Service. Provision permitting the SNO to suspend services until the Participant pays amounts that are due. Failure to pay Service Fees and Miscellaneous

Charges within ___________ (__) days following the due date therefore may result in termination of the Participant's access to the System and/or use of the Services on __________ (__) days prior notice. A reconnection fee equal to ___________________ shall be assessed to reestablish connection after termination due to non-payment.

FC.06 Miscellaneous Fee/Consideration Provisions

pp.05-FC.06
2. For billing purposes, a person will be considered an Immunization Patient in the care of the Provider which (a) most recently accessed the database for information with respect to that person, (b) most recently received a listing of immunizations due including that person without notifying [Entity] that such person was not in the Provider's care, (c) most recently received an individual immunization report for that person without notifying [Entity] that such person was not in the Provider's care; (d) most recently administered an immunization recorded in the [Name] Profile database to that person, or (e) most recently provided immunization and/or demographic information for inclusion in the [Name] Profile database, whichever is latest; provided that a Provider may object to such an identification in writing or electronic message received by [Entity] no later than thirty days from the date of the [Entity] invoice including the identification to which the Provider objects.

pp.05-FC.06
Once an identification has been made and not timely objected to, the Immunization Patient will continue to be considered to be in the care of the Provider until the later of (a) the Immunization Patient's sixth birthday, as shown in the [Name] Profile database or, (b) the last day of the quarter in which an objection to identification which has been accepted by [Entity] was made.

pp.05-FC.06
If the Provider makes a timely objection to the identification of a patient, [Entity] shall have thirty days from the date of its receipt of the objection to request the Provider to state the basis for the objection and provide any information available to the Provider which supports the objection, or accept the objection. If [Entity] does not timely request such statement and verifying information [Entity] will be considered to have accepted the objection and the Provider shall not be liable for any payment to [Entity] with respect to any period after the end of the quarter in which the objection was received by [Entity].

pp.05-FC.06
If [Entity] does timely request such statement and verifying information it shall be forwarded promptly in writing by Provider to [Entity], and [Entity] shall independently verify in its reasonable discretion whether or not the Immunization Patient is still considered to be in the Provider's care. Any of the following will be considered conclusive proof that an Immunization Patient identified with the Provider is still receiving health care from that Provider:

pp.05-FC.06
a. The receipt of compensation from a health plan for the provision of non-emergency health care provided to the Immunization Patient during the quarter in which the Provider's objection is made.

pp.05-FC.06
b. The accessing of the [Name] Profile database for information concerning the Immunization Patient during the quarter in which the Provider's objection is made.

pp.05-FC.06
c. The receipt of a listing showing an immunization due or an individual immunization report for the Immunization Patient without notifying [Entity] that such person was not in the Provider’s care, during the quarter in which the Provider’s objection is made.

pp.05-FC.06
2. For billing purposes, a person will be considered an Immunization Patient in the care of the Provider which (a) most recently accessed the database for information with respect to that person, (b) most recently received a listing of immunizations due including that person without notifying [Entity] that such person was not in the Provider’s care, (c) most recently received an individual immunization report for that person without notifying [Entity] that such person was not in the Provider’s care; (d) most recently administered an immunization recorded in the [Name] Profile database to that person, or (e) most recently provided immunization and/or demographic information for inclusion in the [Name] Profile database, whichever is latest; provided that a Provider may object to such an identification in writing or electronic message received by [Entity] no later than thirty days from the date of the [Entity] invoice including the identification to which the Provider objects.

pp.05-FC.06
Once an identification has been made and not timely objected to, the Immunization Patient will continue to be considered to be in the care of the Provider until the later of (a) the Immunization Patient’s sixth birthday, as shown in the [Name] Profile database or, (b) the last day of the quarter in which an objection to identification which has been accepted by [Entity] was made.

pp.05-FC.06
If the Provider makes a timely objection to the identification of a patient, [Entity] shall have thirty days from the date of its receipt of the objection to request the Provider to state the basis for the objection and provide any information available to the Provider which supports the objection, or accept the objection. If [Entity] does not timely request such statement and verifying information [Entity] will be considered to have accepted the objection and the Provider shall not be liable for any payment to [Entity] with respect to any period after the end of the quarter in which the objection was received by [Entity].

pp.05-FC.06
If [Entity] does timely request such statement and verifying information it shall be forwarded promptly in writing by Provider to [Entity], and [Entity] shall independently verify in its reasonable discretion whether or not the Immunization Patient is still considered to be in the Provider’s care. Any of the following will be considered conclusive proof that an Immunization Patient identified with the Provider is still receiving health care from that Provider:

pp.05-FC.06
The receipt of compensation from a health plan for the provision of non-emergency health care provided to the Immunization Patient during the quarter in which the Provider's objection is made.

pp.05-FC.06
The accessing of the [Name] Profile database for information concerning the Immunization Patient during the quarter in which the Provider's objection is made.

pp.05-FC.06
The receipt of a listing showing an immunization due or an individual immunization report for the Immunization Patient without notifying [Entity] that such person was not in the Provider's care, during the quarter in which the Provider's objection is made.

ph.09-FC.06
12.1 Agreed-Upon Fees. Provision for a Participant’s written agreement to take precedence over the SNO Terms and Conditions.

12.2 Service Fees. The SNO’s fees for Participants.

12.3 Changes to Fee Schedule. Provisions allowing the SNO to change its Fee Schedule.

12.4 Miscellaneous Charges. Provisions addressing the SNO’s ability to charge for additional services.

12.5 Payment. How and when payment is due and payable.

12.6 Late Charges. Whether the SNO would impose late charges on delinquent Service Fees and Miscellaneous Charges.

ph.09-FC.06
12.7 Suspension of Service. Whether the SNO would be permitted to suspend services until the Participant pays amounts that are due.

ph.09-FC.06
12.8 Taxes. The party responsible for payment of taxes arising out of the use of the SNO’s System and/or Services.

ph.06-FC.06
12. Fees and Charges. Terms regarding amounts that the Participant will be required to pay to the SNO in order to use the Services.

ph.06-FC.06
The Model assumes that the SNO will wish to have strict terms regarding payment by Participants. A SNO may wish to adopt measures that are either more or less strict than shown here.

12.8 Taxes. All Service Fees and Miscellaneous Charges shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future, and the Participant shall pay any tax (excluding taxes on [SNO Name]’s net income) that [SNO Name] may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services provided pursuant to the Terms and Conditions.

sp.08-FC.06
Clinic agrees to impose no charge or fee to the patient or client for [IIS] use.

4.11 Confidentiality of Proprietary Information (CP)

CP.01 Scope of Information Covered/Definition

pp.06-CP.01
Section 5.01 Confidentiality. The Participants agree that any Information obtained from the Network will be kept confidential pursuant to the Privacy Rule and all other applicable federal, state, and local laws, statutes and regulations, as well as each Participant's own rules and regulations governing the confidentiality of patient records and information. Participants agree to report promptly to the Management Committee any serious breach of the confidentiality of the Information of which it becomes aware. Any hard copy of patient Information acquired from the Network for Treatment purposes will be placed in the correspondence section of the patient's medical record which is maintained by each Participant.

pp.06-CP.01
Section 5.02 Enforcement of Confidentiality by Participants. Each Participant agrees to enforce the confidentiality provisions of this Agreement by appropriately disciplining individuals within each Participant's organization who violate the confidentiality of the Information pursuant to each Participant's respective confidentiality and disciplinary policies. Such discipline may include, but not be limited to: warnings; suspensions; termination; or modification, suspension, or revocation of medical staff privileges.

pp.06-CP.01
Section 5.03 Access to Participants' Business and Proprietary Data. [Organization] agrees that no data (including aggregate data on a Participant level basis) concerning a Participant will be provided to other Participants or published in an identifiable form without the written permission of the affected Participant. Such data includes, but is not limited to, patient volume, charges to patients or third-party payors and similar reimbursement data, and Participants' practice patterns.

pp.06-CP.01
Section 5.04 Otherwise Permitted Uses of Information. Notwithstanding any other Section of this Agreement, Business Associate may use or disclose for any lawful purpose Information that: (a) is in the possession of Business Associate prior to the time of the disclosure to Business Associate by the Participants and was not acquired, directly or indirectly, from the Participants or the Network; or (b) is made available to Business Associate by a third party who has the legal D.

ph.06-CP.01
As noted above, the parties shall maintain the confidentiality of patient medical records and treatment in accordance with state and federal laws. In addition, each party acknowledges that information regarding the other party's business operations, including, but not limited to, procedures, programs, formularies and reimbursement schedules are proprietary and confidential, and agrees to hold such information in strict confidence and not to disclose or make available such information to any third party, except as required by law.

ph.06-CP.01
13.1 Scope of Proprietary Information. In the performance of their respective responsibilities pursuant to the Terms and Conditions, [SNO Name] and Participants may come into possession of certain Proprietary Information of the other. For the purposes hereof, "Proprietary Information" means all trade secrets, business plans, marketing plans, know-how, data, contracts, documents, scientific and medical concepts, member and

customer lists, costs, financial information, profits and billings, and referral sources, existing or future services, products, operations, management, pricing, financial status, goals, strategies, objectives, and agreements of the Shareholder and the Corporation, whether written or verbal, that are confidential in nature; provided, however, that Proprietary Information shall not include any information that: (a) Is in the public domain; (b) Is already known or obtained by any other party other than in the course of the other party's performance pursuant to the Terms and Conditions; (c) Is independently developed by any other party; and/or (d) Becomes known from an independent source having the right to disclose such information and without similar restrictions as to disclosure and use and without breach of the Terms and Conditions, or any other confidentiality or nondisclosure agreement by such other party.

ss.05-CP.01
"Identifiable data or information" is specific to an individual and may include elements such as demographic information, address, date of birth; etc. Data or information is "Identifiable" if it directly identifies an individual or there is a reasonable basis to believe it could be used to identify an individual, information may also be "identifiable" if it meets the definition as contained in an applicable law. This form of information is defined by applicable federal, provincial and state laws and the definitions in those laws may vary from jurisdiction to jurisdiction;

hh.06-CP.01
7. Confidential Information. Each Network acknowledges that in accessing and using the Exchanges, it will be exposed to and provided with Network confidential information, including but not limited to the Exchange and all related software, documentation, and services provided by Network in establishing and maintaining the Exchange.

C. [Entity]'s Obligation to Maintain Provider Confidentiality:

CP.02 Scope of Allowed/Disallowed Disclosure

pp.05-CP.02
[Entity] may from time to time receive requests from health plans, public health agencies, academic researchers or other interested parties seeking information which may pertain to providers. [Entity] WILL NOT RELEASE ANY INFORMATION IDENTIFYING ANY PROVIDER, OR ANY INDIVIDUAL AFFILIATED WITH ANY PROVIDER WHO HAS SIGNED THIS CONTRACT TO ANY SUCH PARTY WITHOUT THE WRITTEN CONSENT OF THE PROVIDER OR OTHER IDENTIFIED PERSON(S), EXCEPT IN THE EVENT THAT SUCH DISCLOSURE IS REQUIRED BY COURT OR AGENCY ORDER. IN THE EVENT OF SUCH AN ORDER [Entity] WILL CONTEST THE DISCLOSURE AND, UNLESS PROHIBITED BY LAW, SHALL GIVE THE PROVIDER PROMPT NOTICE OF ITS SERVICE. This nondisclosure obligation does not apply to disclosures to other health care providers who have entered into a Health Care Provider Information Sharing Agreement with [Entity], when disclosed as part of the immunization information provided with respect to a particular patient.

pp.05-CP.02
[Entity] may from time to time receive requests from health plans, public health agencies, academic researchers or other interested parties seeking information which may pertain to providers. [Entity] WILL NOT RELEASE ANY INFORMATION IDENTIFYING ANY PROVIDER WHO HAS SIGNED THIS CONTRACT TO ANY SUCH PARTY WITHOUT THE WRITTEN CONSENT OF THE PROVIDER, EXCEPT IN THE EVENT THAT SUCH DISCLOSURE IS REQUIRED BY COURT OR AGENCY ORDER. IN THE EVENT OF SUCH AN ORDER [Entity] WILL CONTEST THE DISCLOSURE AND, UNLESS PROHIBITED BY LAW, SHALL GIVE THE

PROVIDER PROMPT NOTICE OF ITS SERVICE. This nondisclosure obligation does not apply to disclosures to other health care providers who have entered into this contract, when disclosed as part of the immunization information provided with respect to a particular patient.

ph.06-CP.02
2. [State Organization] Access. Patient hereby authorizes [State Organization] (and all providers the Patient has authorized who are participating in the [State Organization] Network) to have access to his/her PHI for the following uses and purposes:

- Treatment of patient.
- Mitigation of a breach of confidentiality or unauthorized access of PHI.
- Payment for healthcare services.
- Auditing and monitoring use of the Network and compliance with the terms and conditions of this Agreement.
- Providing customized summary reports with non-identifying data or statistics as needed for public health or providing audit information, investigation, and general access in accordance with other governmental purposes as required by law.

ph.06-CP.02
As noted above, the parties shall maintain the confidentiality of patient medical records and treatment in accordance with state and federal laws. In addition, each party acknowledges that information regarding the other party’s business operations, including, but not limited to, procedures, programs, formularies and reimbursement schedules are proprietary and confidential, and agrees to hold such information in strict confidence and not to disclose or make available such information to any third party, except as required by law.

ph.06-CP.02
13.2 Nondisclosure of Proprietary Information. [SNO Name] and the Participant each (i) shall keep and maintain in strict confidence all Proprietary Information received from the other, or from any of the other’s employees, accountants, attorneys, consultants, or other agents and representatives, in connection with the performance of their respective obligations under the Terms and Conditions; (ii) shall not use, reproduce, distribute or disclose any such Proprietary Information except as permitted by the Terms and Conditions; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure.

hh.06-CP.02
Each Network must maintain the confidentiality of such information and materials pursuant to the terms and conditions of this Agreement, and each Network agrees to exercise no less than reasonable care when handling the confidential information. Except as provided in this Agreement, no Network shall disclose the confidential information to a third party without the express written consent of the other Network, unless: (a) a Network is required to do so by law, (b) the confidential information becomes publicly available, or (c) the Network obtained the confidential information prior to the Effective Date of this Agreement, or obtains that information through another source who had no duty of confidentiality to a Network.

ph.06-CP.02
Confidential Information. Hospital acknowledges that in accessing and using the Exchange, it will be exposed to and provided with Access Provider confidential information, including

but not limited to the Exchange and all related software, documentation, and services provided by Access Provider in establishing and maintaining the Exchange. Hospital must maintain the confidentiality of such information and materials pursuant to the terms and conditions of this Agreement, and Hospital agrees to exercise no less than reasonable care when handling the Access Provider confidential information. Except as provided in this Agreement, Hospital shall not disclose the Access Provider confidential information to a third party without the express written consent of Access Provider, unless: (a) Hospital is required to do so by law, (b) the Access Provider confidential information becomes publicly available, or (c) Hospital obtained the Access Provider confidential information prior to the Effective Date of this Agreement, or obtains that information through another source who had no duty of confidentiality to Access Provider

CP.03 Remedies

ph.06-CP.03
13.3 Equitable Remedies. All Proprietary Information represents a unique intellectual product of the party disclosing such Proprietary Information (the “Disclosing Party”). The unauthorized disclosure of said Proprietary Information would have a detrimental impact on the Disclosing Party. The damages resulting from said detrimental impact would be difficult to ascertain but would result in irreparable loss. It would require a multiplicity of actions at law and in equity in order to seek redress against the receiving party in the event of such an unauthorized disclosure. The Disclosing Party shall be entitled to equitable relief in preventing a breach of this Section 13 (Proprietary Information) and such equitable relief is in addition to any other rights or remedies available to the Disclosing Party.

CP.04 Miscellaneous Confidentiality Provisions

ph.06-CP.04
As noted above, the parties shall maintain the confidentiality of patient medical records and treatment in accordance with state and federal laws. In addition, each party acknowledges that information regarding the other party’s business operations, including, but not limited to, procedures, programs, formularies and reimbursement schedules are proprietary and confidential, and agrees to hold such information in strict confidence and not to disclose or make available such information to any third party, except as required by law.

ph.06-CP.04
13. Proprietary Information. Provisions concerning the parties’ respective obligations to preserve the confidentiality of others’ proprietary information (i.e., other than health information).

ph.06-CP.04
13.4 Notice of Disclosure. Notwithstanding any other provision hereof, nothing in this Section 13 (Proprietary Information) shall prohibit or be deemed to prohibit a party hereto from disclosing any Proprietary Information (or any other information the disclosure of which is otherwise prohibited hereunder) to the extent that such party becomes legally compelled to make such disclosure by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction, and such disclosures are expressly permitted hereunder; provided, however, that a party that has been requested or becomes legally compelled to make a disclosure otherwise prohibited hereunder by reason of a subpoena or order of a court, administrative agency or other governmental body of competent jurisdiction shall provide the other party with notice thereof within five (5) calendar days, or, if sooner, at least three (3) business days before such disclosure will be made so that the other party may seek a protective order or other

appropriate remedy. In no event shall a party be deemed to be liable hereunder for compliance with any such subpoena or order of any court, administrative agency or other governmental body of competent jurisdiction.

ph.06-CP.04
Term and Termination. This Agreement shall commence on the Effective Date and shall continue in effect for five (5) years. Either party may terminate this Agreement by providing the other party with ninety (90) days written notice of such termination. Upon termination, all licenses granted to Hospital relating to access to or use of the Exchange or the accompanying software tools and documentation will cease. Upon termination, Hospital promptly shall return all Access Provider confidential information to Network.

ph.06-CP.04
Confidential Information. Hospital acknowledges that in accessing and using the Exchange, it will be exposed to and provided with Access Provider confidential information, including but not limited to the Exchange and all related software, documentation, and services provided by Access Provider in establishing and maintaining the Exchange. Hospital must maintain the confidentiality of such information and materials pursuant to the terms and conditions of this Agreement, and Hospital agrees to exercise no less than reasonable care when handling the Access Provider confidential information. Except as provided in this Agreement, Hospital shall not disclose the Access Provider confidential information to a third party without the express written consent of Access Provider, unless: (a) Hospital is required to do so by law, (b) the Access Provider confidential information becomes publicly available, or (c) Hospital obtained the Access Provider confidential information prior to the Effective Date of this Agreement, or obtains that information through another source who had no duty of confidentiality to Access Provider

4.12 Disclaimers (DI)

DI.01 Disclaimers Regarding Use of Network

ph.06-DI.01
Liability. [State Organization] makes every effort to protect the confidentiality and privacy of Patient health information. In addition, [State Organization] has implemented policies, procedures and technical protections to further limit unauthorized access to Patient information. Accordingly, Patient for himself and his successors in interest, assigns, heirs, agents, trustees and representatives, does unequivocally discharge and forever release [State Organization], its directors, staff, or employees from any and all liability, claims (legal, equitable, administrative or otherwise) and damages he/she could have alleged against [State Organization], including but not limited to liability, claims and damages related to [State Organization]’s delivery of Patient’s medical records.

ph.06-DI.01
14.1 Carrier Lines. By using the System and the Services, each Participant shall acknowledge that access to the System is to be provided over various facilities and communications lines, and information will be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, “carrier lines”) owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which are beyond [SNO name]’s control. [SNO Name] assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information

attributable to transmission on the carrier lines. Use of the carrier lines is solely at user's risk and is subject to all applicable local, state, national, and international laws.

ph.06-DI.01
Disclaimers. Network provides the Exchange "as is" and without any warranty of any kind to Hospital, whether express, implied, or statutory. Network does not warrant that the performance or delivery of the Exchange will be uninterrupted or error-free. Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Network shall not be liable to Hospital for any consequential, incidental, indirect, punitive, or special damages suffered by Hospital or any other third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. Network shall not be liable for any damages arising out of or related to the acts or omissions of Hospital in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

ph.06-DI.01
Liability. [State Organization] makes every effort to protect the confidentiality and privacy of Patient health information. In addition, [State Organization] has implemented policies, procedures and technical protections to further limit unauthorized access to Patient information. Accordingly, Patient for himself and his successors in interest, assigns, heirs, agents, trustees and representatives, does unequivocally discharge and forever release [State Organization], its directors, staff, or employees from any and all liability, claims (legal, equitable, administrative or otherwise) and damages he/she could have alleged against [State Organization], including but not limited to liability, claims and damages related to [State Organization]'s delivery of Patient's medical records.

ph.06-DI.01
Data. Hospital acknowledges that the information provided through the Exchange is drawn from numerous sources, and Hospital and its employees agree to verify, to the best of their ability, that the Data obtained from Exchange which Hospital's employees rely upon in making treatment decisions about each patient in fact corresponds to that patient. Hospital agrees and understands that the Data accessed through Exchange may not include a patient's entire record of treatment in the region. Hospital shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data. Hospital shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

ph.06-DI.01
Hospital acknowledges and agrees that the Exchange: (a) is accessed over the Internet; (b) relies, in part, on the existence and proper operation of equipment and software that is outside of the control of Network, Access Provider, and/or Host; and (c) relies on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by Hospital may be prevented by events or actions outside of Network's, Access Provider's, and/or Host's control. Network, Access Provider, and Host have made and hereby make no guarantee or warranty to Hospital as to the availability or accessibility of the Exchange or Data.

ph.06-DI.01
14.4 Participant's Actions. The Participant shall be solely responsible for any damage to a computer system, loss of data, and any damage to the System caused by that Participant or

any person using a user ID assigned to the Participant or a member of the Participant's workforce.

hh.06-DI.01
3.3 Lack of Guarantee or Warranty. Each Network acknowledges and agrees that the Exchanges: (a) are accessed over the Internet; (b) rely, in part, on the existence and proper operation of equipment and software that is outside of the control of Networks and Authorized Users; and (c) rely on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by a Network may be prevented by events or actions outside of the other Network's or Authorized User's control. The Networks and Authorized Users have made and hereby make no guarantee or warranty to each other as to the availability or accessibility of the Exchanges or Data.

sp.02-DI.01
d. Neither the [Program] Management Committee nor [Entity] shall be liable for any general, special, consequential or other damages which may arise or be claimed to arise from any use of information by the Participant and/or the Participant's employees, contractors, officers, agents, or other affiliated or associated persons. The Participant is solely responsible for ensuring the exercise of independent professional judgment in the use of any information received under this Agreement.

DI.02 Disclaimers Regarding Quality, Accuracy, Completeness, Timing, etc. of Services or Data

ph.06-DI.02
14.5 Unauthorized Access; Lost or Corrupt Data. [SNO Name] is not responsible for unauthorized access to the Participant's transmission facilities or equipment by individuals or entities using the System or for unauthorized access to, or alteration, theft, or destruction of the participant's data files, programs, procedures, or information through the System, whether by accident, fraudulent means or devices, or any other method. The Participant is solely responsible for validating the accuracy of all output and reports and protecting the Participant's data and programs from loss by implementing appropriate security measures, including routine backup procedures. The Participant waives any damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, or the use of third-party software. [SNO Name] is not responsible for the content of any information transmitted or received through [SNO name]'s provision of the Services.

ph.06-DI.02
14.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service

resulting from communication failures by telecommunication service providers or the System.

sp.02-DI.02
c. The [Program] Management Committee and [Entity] cannot and do not guarantee the truth, accuracy, or completeness of any information provided under this Agreement but shall use reasonable efforts to ensure the integrity of the information received, processed and disclosed through the [Program] Cardiac Registry.

hh.06-DI.02
Neither Network warrants that the performance or delivery of the Exchange will be uninterrupted or error-free.

hh.06-DI.02
Each Network agrees and understands that the Data accessed through the Exchanges may not include a patient's entire record of treatment in the region.

ph.06-DI.02
Hospital acknowledges and agrees that the Exchange: (a) is accessed over the Internet; (b) relies, in part, on the existence and proper operation of equipment and software that is outside of the control of Network, Access Provider, and/or Host; and (c) relies on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by Hospital may be prevented by events or actions outside of Network's, Access Provider's, and/or Host's control. Network, Access Provider, and Host have made and hereby make no guarantee or warranty to Hospital as to the availability or accessibility of the Exchange or Data**.**

ph.06-DI.02
Data. Hospital acknowledges that the information provided through the Exchange is drawn from numerous sources, and Hospital and its employees agree to verify, to the best of their ability, that the Data obtained from Exchange which Hospital's employees rely upon in making treatment decisions about each patient in fact corresponds to that patient. Hospital agrees and understands that the Data accessed through Exchange may not include a patient's entire record of treatment in the region. Hospital shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data. Hospital shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

ph.06-DI.02
Disclaimers. Network provides the Exchange "as is" and without any warranty of any kind to Hospital, whether express, implied, or statutory. Network does not warrant that the performance or delivery of the Exchange will be uninterrupted or error-free. Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Network shall not be liable to Hospital for any consequential, incidental, indirect, punitive, or special damages suffered by Hospital or any other third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. Network shall not be liable for any damages arising out of or related to the acts or omissions of Hospital in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

ph.06-DI.02
Liability. [State Organization] makes every effort to protect the confidentiality and privacy of Patient health information. In addition, [State Organization] has implemented policies, procedures and technical protections to further limit unauthorized access to Patient information. Accordingly, Patient for himself and his successors in interest, assigns, heirs, agents, trustees and representatives, does unequivocally discharge and forever release [State Organization], its directors, staff, or employees from any and all liability, claims (legal, equitable, administrative or otherwise) and damages he/she could have alleged against [State Organization], including but not limited to liability, claims and damages related to [State Organization]'s delivery of Patient's medical records.

mm.04-DI.02
Acceptance by Users as Ultimate Operational Test of Record
Requirements for Acceptance by Users
Confidence in the technology and database manager
Right to rely on data sources
Readily accessible and easily understood interface

hh.06-DI.02
Each Network provides access to its Exchange "as is" and without any warranty of any kind whether express, implied, or statutory.

hh.06-DI.02
Neither Network warrants that the performance or delivery of the Exchange will be uninterrupted or error-free.

ph.06-DI.02
14.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

ph.06-DI.02
14.6 Inaccurate Data. All data to which access is made through the System and/or the Services originates from Data Providers and other parties making data available through the NHIN, and not from [SNO Name]. All such data is subject to change arising from numerous factors, including without limitation, changes to patient health information made at the request of the patient, changes in the patient's health condition, the passage of time and other factors. [SNO Name] neither initiates the transmission of any data nor monitors the specific content of data being transmitted. Without limiting any other provision of the Terms and Conditions, [SNO Name] shall have no responsibility for or liability related to the

accuracy, content, currency, completeness, content, or delivery of any data either provided by a Data Provider, or used by a Data Recipient, pursuant to the Terms and Conditions.

ph.02-DI.02
PROVIDER/REPOSITORY makes any representations or warranties with respect to the completeness, quality or suitability of any data for purposes of this Agreement, or the possible presence of computer worms, viruses or other malicious code in any data. All data shall be made available "as is" and at RESEARCHER's sole risk.

ph.06-DI.02
Liability. [State Organization] makes every effort to protect the confidentiality and privacy of Patient health information. In addition, [State Organization] has implemented policies, procedures and technical protections to further limit unauthorized access to Patient information. Accordingly, Patient for himself and his successors in interest, assigns, heirs, agents, trustees and representatives, does unequivocally discharge and forever release [State Organization], its directors, staff, or employees from any and all liability, claims (legal, equitable, administrative or otherwise) and damages he/she could have alleged against [State Organization], including but not limited to liability, claims and damages related to [State Organization]'s delivery of Patient's medical records.

DI.03 Disclaimers Regarding Actions/Omissions of Other Participants

ph.06-DI.03
Hospital acknowledges and agrees that the Exchange: (a) is accessed over the Internet; (b) relies, in part, on the existence and proper operation of equipment and software that is outside of the control of Network, Access Provider, and/or Host; and (c) relies on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by Hospital may be prevented by events or actions outside of Network's, Access Provider's, and/or Host's control. Network, Access Provider, and Host have made and hereby make no guarantee or warranty to Hospital as to the availability or accessibility of the Exchange or Data**.**

ph.06-DI.03
Data. Hospital acknowledges that the information provided through the Exchange is drawn from numerous sources, and Hospital and its employees agree to verify, to the best of their ability, that the Data obtained from Exchange which Hospital's employees rely upon in making treatment decisions about each patient in fact corresponds to that patient. Hospital agrees and understands that the Data accessed through Exchange may not include a patient's entire record of treatment in the region. Hospital shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data. Hospital shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

ph.06-DI.03
14.3 Other Participants. By using the System and the Services, each Participant shall acknowledge that other Participants have access to the System and Services, and that other parties have access to the information contained in the System through their participation in the NHIN. Such other Participants have agreed to comply with the Common Framework Policies and Procedures, concerning use of the information made available through the NHIN; however, the actions of such other parties are beyond the control of [SNO Name]. Accordingly, [SNO Name] does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on the System resulting from any Participant's actions or failures to act.

DI.04 Disclaimers Regarding Patient Care

ph.06-DI.04
14.7 Patient Care. Without limiting any other provision of the Terms and Conditions, the Participant and the Participant's Authorized Users shall be solely responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients and clients resulting from or in any way related to the use of the System or the Services or the data made available thereby. No Participant or Authorized User shall have any recourse against, and through the Registration Agreements that apply thereto, each shall waive, any claims against [SNO Name] for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of the System and/or the Services or the data made available thereby.

DI.05 Disclaimers Regarding Participant's Use of Data

ph.06-DI.05
14.4 Participant's Actions. The Participant shall be solely responsible for any damage to a computer system, loss of data, and any damage to the System caused by that Participant or any person using a user ID assigned to the Participant or a member of the Participant's workforce.

mm.04-DI.05
Acceptance by Users as Ultimate Operational Test of Record
Requirements for Acceptance by Users
Confidence in the technology and database manager
Right to rely on data sources
Readily accessible and easily understood interface

ph.06-DI.05
14.6 Inaccurate Data. All data to which access is made through the System and/or the Services originates from Data Providers and other parties making data available through the NHIN, and not from [SNO Name]. All such data is subject to change arising from numerous factors, including without limitation, changes to patient health information made at the request of the patient, changes in the patient's health condition, the passage of time and other factors. [SNO Name] neither initiates the transmission of any data nor monitors the specific content of data being transmitted. Without limiting any other provision of the Terms and Conditions, [SNO Name] shall have no responsibility for or liability related to the accuracy, content, currency, completeness, content, or delivery of any data either provided by a Data Provider, or used by a Data Recipient, pursuant to the Terms and Conditions.

ph.06-DI.05
Data. Hospital acknowledges that the information provided through the Exchange is drawn from numerous sources, and Hospital and its employees agree to verify, to the best of their ability, that the Data obtained from Exchange which Hospital's employees rely upon in making treatment decisions about each patient in fact corresponds to that patient. Hospital agrees and understands that the Data accessed through Exchange may not include a patient's entire record of treatment in the region. Hospital shall establish and implement appropriate policies and procedures for purposes of preventing unauthorized access to and disclosure of Data. Hospital shall protect the confidentiality of all Data in accordance with applicable laws and the terms and conditions of this Agreement.

ph.06-DI.05
14.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

DI.06 Limitation on HIE Liability

ph.06-DI.06
14.3 Other Participants. By using the System and the Services, each Participant shall acknowledge that other Participants have access to the System and Services, and that other parties have access to the information contained in the System through their participation in the NHIN. Such other Participants have agreed to comply with the Common Framework Policies and Procedures, concerning use of the information made available through the NHIN; however, the actions of such other parties are beyond the control of [SNO Name]. Accordingly, [SNO Name] does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on the System resulting from any Participant's actions or failures to act.

ph.06-DI.06
14.1 Carrier Lines. By using the System and the Services, each Participant shall acknowledge that access to the System is to be provided over various facilities and communications lines, and information will be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which are beyond [SNO name]'s control. [SNO Name] assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at user's risk and is subject to all applicable local, state, national, and international laws.

ph.06-DI.06
14.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data,

whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

ph.06-DI.06
14.5 Unauthorized Access; Lost or Corrupt Data. [SNO Name] is not responsible for unauthorized access to the Participant's transmission facilities or equipment by individuals or entities using the System or for unauthorized access to, or alteration, theft, or destruction of the participant's data files, programs, procedures, or information through the System, whether by accident, fraudulent means or devices, or any other method. The Participant is solely responsible for validating the accuracy of all output and reports and protecting the Participant's data and programs from loss by implementing appropriate security measures, including routine backup procedures. The Participant waives any damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, or the use of third-party software. [SNO Name] is not responsible for the content of any information transmitted or received through [SNO name]'s provision of the Services.

ph.06-DI.06
14.8 Limitation of Liability. Notwithstanding anything in the Terms and Conditions to the contrary, to the maximum extent permitted by applicable laws, the aggregate liability of [SNO Name], and [SNO Name]'s officers, directors, employees, and other agents, under any Participant's Registration Agreement, regardless of theory of liability, shall be limited to the aggregate fees actually paid by the Participant in accordance with the Terms and Conditions for the six- (6) month period preceding the event first giving rise to the claim.

hh.06-DI.06
Each Network provides access to its Exchange "as is" and without any warranty of any kind whether express, implied, or statutory.

hh.06-DI.06
Each Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Neither Network shall be liable to the other for any consequential, incidental, indirect, punitive, or special damages suffered by a Network or any third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. No Network shall be liable for any damages arising out of or related to the acts or omissions of a Network in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

ph.06-DI.06
5.5 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users. The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant's Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant's Authorized Users, with respect to the System, the Services and/or any confidential and/or

other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant. 14. Disclaimers, Exclusions of Warranties, Limitations of Liability, and Indemnifications. Standard terms directed to avoiding inappropriate legal claims between the parties. The specific language shown in this section is for illustration only. The SNO would need to tailor the language of this section to comply with applicable state laws regarding the content and presentation (e.g., capital letters) of disclaimers and limitations of warranties and similar issues.

ph.06-DI.06
Disclaimers. Network provides the Exchange "as is" and without any warranty of any kind to Hospital, whether express, implied, or statutory. Network does not warrant that the performance or delivery of the Exchange will be uninterrupted or error-free. Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Network shall not be liable to Hospital for any consequential, incidental, indirect, punitive, or special damages suffered by Hospital or any other third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. Network shall not be liable for any damages arising out of or related to the acts or omissions of Hospital in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

DI.07 Miscellaneous Disclaimer Provisions

ph.06-DI.07
14.2 No Warranties. Access to the System, use of the Services, and the information obtained by a Data Recipient pursuant to the use of those services are provided "as is" and "as available" without any warranty of any kind, expressed or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. The Participant is solely responsible for any and all acts or omissions taken or made in reliance on the System or the information in the System, including inaccurate or incomplete information. It is expressly agreed that in no event shall [SNO Name] be liable for any special, indirect, consequential, or exemplary damages, including but not limited to, loss of profits or revenues, loss of use, or loss of information or data, whether a claim for any such liability or damages is premised upon breach of contract, breach of warranty, negligence, strict liability, or any other theories of liability, even if [SNO Name] has been apprised of the possibility or likelihood of such damages occurring. [SNO Name] disclaims any and all liability for erroneous transmissions and loss of service resulting from communication failures by telecommunication service providers or the System.

ph.06-DI.07
14.1 Carrier Lines. By using the System and the Services, each Participant shall acknowledge that access to the System is to be provided over various facilities and communications lines, and information will be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which are beyond [SNO name]'s control. [SNO Name] assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at user's risk and is subject to all applicable local, state, national, and international laws.

ph.06-DI.07
14.5 Unauthorized Access; Lost or Corrupt Data. [SNO Name] is not responsible for unauthorized access to the Participant's transmission facilities or equipment by individuals or entities using the System or for unauthorized access to, or alteration, theft, or destruction of the participant's data files, programs, procedures, or information through the System, whether by accident, fraudulent means or devices, or any other method. The Participant is solely responsible for validating the accuracy of all output and reports and protecting the Participant's data and programs from loss by implementing appropriate security measures, including routine backup procedures. The Participant waives any damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, or the use of third-party software. [SNO Name] is not responsible for the content of any information transmitted or received through [SNO name]'s provision of the Services.

ph.06-DI.07
Hospital acknowledges and agrees that the Exchange: (a) is accessed over the Internet; (b) relies, in part, on the existence and proper operation of equipment and software that is outside of the control of Network, Access Provider, and/or Host; and (c) relies on access to information from, and the provision of information controlled by, third-parties and, as a result, access to the Data by Hospital may be prevented by events or actions outside of Network's, Access Provider's, and/or Host's control. Network, Access Provider, and Host have made and hereby make no guarantee or warranty to Hospital as to the availability or accessibility of the Exchange or Data**.**

ph.06-DI.07
Disclaimers. Network provides the Exchange "as is" and without any warranty of any kind to Hospital, whether express, implied, or statutory. Network does not warrant that the performance or delivery of the Exchange will be uninterrupted or error-free. Network hereby disclaims all implied and express warranties, conditions, and other terms, whether statutory, arising from course of dealing, or otherwise, including without limitation terms as to merchantability or fitness for a particular purpose. Network shall not be liable to Hospital for any consequential, incidental, indirect, punitive, or special damages suffered by Hospital or any other third party, however caused and regardless of legal theory or foreseeability, including, without limitation, lost profits, business interruptions, or other economic loss, directly or indirectly arising out of this Agreement. Network shall not be liable for any damages arising out of or related to the acts or omissions of Hospital in (a) accessing or using the Exchange or (b) disclosing any Data contained therein.

pp.06-DI.07
Section 6.04 Disclaimer of Warranties. Although all equipment associated with the Network that is supplied by [Organization] (or that was previously supplied by [State] University or [Organization] pursuant to the First Agreement) shall remain the property of NLM or [Organization] (as applicable) and the Parties do not intend for the provision of the equipment to constitute a sale or lease under the [State] Uniform Commercial Code, the Participants nevertheless acknowledge that any equipment associated with the Network provided to the Participants by [Organization] (or that was previously supplied by [State] University or [Organization] pursuant to the First Agreement) is provided AS IS WITH ALL FAULTS. [ORGANIZATION] HEREBY DISCLAIMS ANY WARRANTIES, WHETHER EXPRESS OR IMPLIED, WHICH MAY BE CLAIMED REGARDING ANY OF THE EQUIPMENT SUPPLIED TO THE PARTICIPANTS. [ORGANIZATION] SPECIFICALLY HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The Participants agree to hold harmless [Organization] for any failure of any hardware,

commercial software, communication lines, or other equipment supplied by [Organization] for use in connection with the Network or for the failure to supply or maintain said equipment. [Organization] shall take all reasonable steps to assure that manufacturers' and sellers' warranties may be enforced by the Participants, and shall cooperate with the Participants in exercising warranty rights.

ph.06-DI.07
5.5 Responsibility for Conduct of Participant and Authorized Users. The Participant's responsibility for the conduct of its Authorized Users. The Participant shall be solely responsible for all acts and omissions of the Participant and/or the Participant's Authorized Users, and all other individuals who access the System and/or use the Services either through the Participant or by use of any password, identifier or log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant's Authorized Users, with respect to the System, the Services and/or any confidential and/or other information accessed in connection therewith, and all such acts and omissions shall be deemed to be the acts and omissions of the Participant.

14. Disclaimers, Exclusions of Warranties, Limitations of Liability, and Indemnifications. Standard terms directed to avoiding inappropriate legal claims between the parties. The specific language shown in this section is for illustration only. The SNO would need to tailor the language of this section to comply with applicable state laws regarding the content and presentation (e.g., capital letters) of disclaimers and limitations of warranties and similar issues.

4.13 Insurance (IN)

IN.01 Participant Requirement

ph.06-IN.01
In order to adequately insure themselves for liability arising out of the activities to be performed under this Agreement, each party agrees to obtain and maintain in force and effect liability insurance to insure themselves and their respective personnel for liability arising out of activities to be performed under, or in any manner related to, this Agreement.

ph.06-IN.01
15. Insurance and Indemnification.

15.1 Insurance. Requirements that Participants have appropriate insurance coverage. The Participant shall obtain and maintain insurance coverage in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also comply with the insurance requirements described below:]

IN.02 HIE Requirement

ph.06-IN.02
In order to adequately insure themselves for liability arising out of the activities to be performed under this Agreement, each party agrees to obtain and maintain in force and effect liability insurance to insure themselves and their respective personnel for liability arising out of activities to be performed under, or in any manner related to, this Agreement.

hh.06-IN.02
3.5 Insurance. Each Network shall obtain and maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $__________ each occurrence. If such insurance contains a general aggregate limit, it shall apply separately to this contract or be no less than two times the occurrence limit.

IN.03 Miscellaneous Insurance Provisions

ph.06-IN.03
15. Insurance and Indemnification.

15.1 Insurance. Requirements that Participants have appropriate insurance coverage. The Participant shall obtain and maintain insurance coverage in accordance with the Common Framework Policies and Procedures, which is incorporated herein by reference. [Optional: Without limiting the generality of the foregoing, the Participant shall also comply with the insurance requirements described below:]

sp.04-IN.03
Maintain the following insurance:

Commercial General Liability Insurance: Participating Clinic shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than $2,000,000 each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this contract or be no less than two times the occurrence limit.

Professional Liability Insurance: Participating Clinic shall obtain and maintain general professional liability insurance with a limit of not less than $1,000,000 per each occurrence and $3,000,000 in the aggregate. If such insurance is provided on a claims made basis, then Participating Clinic shall provide “tail” coverage for a period of five years after the termination of coverage.

Workers’ Compensation Insurance: Participating Clinic shall procure and maintain workers’ compensation and employers’ liability insurance as required by [State] law.

Certificates of Insurance: Prior to commencement of work under this Agreement, Participating Clinic shall furnish [Program] properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and promptly provide updated Certificates of Insurance on an ongoing basis. Such insurance shall not be canceled, except on 30 days’ prior written notice to [Program]. Participating Clinic shall furnish copies of insurance policies if requested by State.

4.14 Indemnification (IM)

IM.01 Indemnification of Participant

pp.06-IM.01
Section 9.01 Indemnification by Participants. A Participant that breaches the confidentiality of the Information, or submits inaccurate, incomplete, or defamatory data to the Network (“Breaching Participant”) agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought (“Sued Party”) by any individual arising out of or resulting from such breach of confidentiality or submission of inaccurate, incomplete, or defamatory data by the Breaching Participant or any individual for whom such Participant is responsible. Such indemnification shall include the payment of all costs associated with

defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against the Sued Party arising out of or resulting from any breach of confidentiality of the Information, or the submission of inaccurate, incomplete, or defamatory data to the Network by the Breaching Participant or any individual for whom such Participant is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, the Breaching Participant, at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to the Breaching Participant within a period wherein the Breaching Participant is not prejudiced by lack of such notice. If the Breaching Participant is required to indemnify and defend, it will thereafter have control of such litigation, but the Breaching Participant may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably withheld. This Section is not, as to third parties, a waiver of any defense or immunity otherwise available to the Sued Party; and the Breaching Participant, in defending any action on behalf of the Sued Party, shall be entitled to assert in any action every defense or immunity that the Sued Party could assert in its own behalf.

ph.06-IM.01
15.2.1. Generally.

Alternative One: Provisions requiring the parties to indemnify each other for losses caused by claims by third parties.

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

ph.06-IM.01
OR Alternative Two: Provisions requiring the parties to indemnify each other as well as requiring Participants to indemnify each other:

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other and, if the Participant is the Indemnifying Party, the other Participants (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

ph.06-IM.01
15.2.2 Specific Indemnities.

Provisions calling for special indemnification terms.

Alternative One: SNO and Participant indemnify each other for Serious Breaches of Confidentiality or Security for which they are responsible.

Notwithstanding Section 15.2.1 (Generally), [SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of any Serious Breach of Confidentiality or Security arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees.

mm.10-IM.01
Indemnification of providers against lawsuits for data they publish that is misused by a user from a consuming system**.**

mm.10-IM.01
Recourse methods for providers to communicate problems with published data, rather than the use of that data.

IM.02 Indemnification of the HIE

pp.06-IM.02
Section 9.02 Indemnification by [Organization]. [Organization] agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought ("Sued Party") by any individual arising out of or resulting from any breach of confidentiality of the Information (whether through disclosure or through acts or omissions in the design and/or maintenance of the Network) by [Organization] or any individual for whom [Organization] is responsible. Such indemnification shall include the payment of all costs associated with defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against any Sued Party arising out of or resulting from a breach of confidentiality of the Information by [Organization] or any individual for whom [Organization] is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, [Organization], at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to [Organization] within a period wherein [Organization] is not prejudiced by lack of such notice. If [Organization] is required to indemnify and defend, it will thereafter have control of such litigation, but [Organization] may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably withheld. This Section is not, as to third parties, a waiver of any defense or immunity otherwise available to the Sued Party; and [Organization], in defending any action on behalf of the Sued Party, shall be entitled to assert in any action every defense or immunity that the Sued Party could assert in its own behalf.

ph.06-IM.02
Liability. [State Organization] makes every effort to protect the confidentiality and privacy of Patient health information. In addition, [State Organization] has implemented policies, procedures and technical protections to further limit unauthorized access to Patient information. Accordingly, Patient for himself and his successors in interest, assigns, heirs, agents, trustees and representatives, does unequivocally discharge and forever release [State Organization], its directors, staff, or employees from any and all liability, claims (legal, equitable, administrative or otherwise) and damages he/she could have alleged against [State Organization], including but not limited to liability, claims and damages related to [State Organization]'s delivery of Patient's medical records.

ph.06-IM.02
15.2.1. Generally.

Alternative One: Provisions requiring the parties to indemnify each other for losses caused by claims by third parties.

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

ph.06-IM.02
OR Alternative Two: Provisions requiring the parties to indemnify each other as well as requiring Participants to indemnify each other:

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other and, if the Participant is the Indemnifying Party, the other Participants (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

ph.06-IM.02
15.2.2 Specific Indemnities.

Provisions calling for special indemnification terms.

Alternative One: SNO and Participant indemnify each other for Serious Breaches of Confidentiality or Security for which they are responsible.

Notwithstanding Section 15.2.1 (Generally), [SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of any Serious Breach of Confidentiality or Security arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees.

ph.06-IM.02
AND/OR Alternative Two: Data Provider indemnifies SNO for losses caused by the Data Provider's provision of inaccurate data.

Notwithstanding Section 15.2.1 (Generally), a Data Provider shall hold [SNO Name] free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of Data Provider's provision of any Patient Data that is inaccurate, incomplete, or defamatory.

ph.06-IM.02
Indemnification. Hospital will indemnify and hold Network and its employees, agents, subcontractors, and licensors harmless from and against any and all liability (including reasonable attorney's fees), injury, or damages that arise from or are related to: (a) Hospital's use of or inability to use the Exchange; or (b) Hospital's breach of this

Agreement, including, without limitation, Hospital's breach of any obligation, representation, or warranty set forth herein.

sp.08-IM.02
Clinic agrees to hold harmless and indemnify the State of [State], its officers, agent and employees, from and against any and all actions, suits, damages, liability or other proceeding which may arise as a result of performing services hereunder. This section does not require Clinic to be responsible for or defend against claims or damages arising solely form acts or omissions of State, its officers or employees.

IM.03 Participant's Indemnification of Other Participants

ph.02-IM.03
13. Indemnification. RESEARCHER shall indemnify, hold harmless and defend PROVIDER/ REPOSITORY and the Data Provider from and against any penalties, claims or damages arising from or pertaining to a breach of this Agreement, or the violation of any federal or state law applicable to the use, disclosure or protection of data subject to this Agreement by RESEARCHER or any of its authorized contractors, agents or employees.

ph.06-IM.03
OR Alternative Two: Provisions requiring the parties to indemnify each other as well as requiring Participants to indemnify each other:

[SNO Name] and each Participant (each, an "Indemnifying Party") each shall hold the other and, if the Participant is the Indemnifying Party, the other Participants (the "Indemnified Party") free of and harmless from all liability, judgments, costs, damages, claims, or demands, including reasonable attorneys' fees, net of the proceeds of insurance, arising out of the act or omission of the Indemnifying Party or any of the Indemnifying Party's Authorized Users, members, agents, staff, or employees, including the Indemnifying Party's failure to comply with or perform its obligations under the applicable Registration Agreement.

hh.06-IM.03
Indemnification. Each Network will indemnify and hold the other and its employees, agents, subcontractors, and licensors harmless from and against any and all liability (including reasonable attorneys' fees), injury, or damages that arise from or are related to: (a) a Network's use of or inability to use an Exchange; or (b) Network's breach of this Agreement, including, without limitation, Network's breach of any obligation, representation, or warranty set forth herein.

mm.10-IM.03
Mechanism to isolate financial responsibility to a particular provider when a patient sues another for misuse of his or her data.

sp.04-IM.03
Hold harmless and indemnify the State of [State], its officers, agents, and employees, from and against any and all actions, suits, damages, liability, or other proceedings which may arise as a result of performing services hereunder. This section does not require Participating Clinic to be responsible for or defend against claims or damages arising solely from acts or omissions of State, its officers, agents, or employees.

IM.04 Miscellaneous Indemnification Provisions

mm.04-IM.04
Mutual Indemnification Provisions
Provisions for Mandatory Increases in Security Measures to Meet Evolving Standards

ph.06-IM.04
OR
Alternative Three: Making no special provision for indemnification, but allowing the parties' existing legal obligations to remain in effect.

Nothing in the Terms and Conditions or any Registration Agreement shall limit [SNO Name]'s or a Participant's respective legal and equitable obligations to each other and to other Participants arising out of the doctrines of equitable indemnity, comparative negligence, contribution or other common law bases of liability.

ph.06-IM.04
The SNO may choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information, or a Data Provider's provision of inaccurate data. The provisions shown here are provided as examples.

ph.06-IM.04
15.2.3 Rules for Indemnification.

Provisions governing the parties' indemnification obligations.

Any indemnification made pursuant to the Terms and Conditions shall include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys' fees and any settlement by or judgment against the party to be indemnified. In the event that a lawsuit is brought against the party to be indemnified, the party responsible to indemnify that party shall, at its sole cost and expense, defend the party to be indemnified, if the party to be indemnified demands indemnification by written notice given to the indemnifying party within a period of time wherein the indemnifying party is not prejudiced by lack of notice. Upon receipt of such notice, the indemnifying party shall have control of such litigation but may not settle such litigation without the express consent of the party to be indemnified, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third parties, be a waiver of any defense or immunity otherwise available, and the indemnifying party, in indemnifying the indemnified party, shall be entitled to assert in any action every defense or immunity that the indemnified party could assert on its own behalf.

mm.10-IM.04
Liability and Risk Allocation

Distinguish any policies regarding liability issues and risk allocation for the XDS Affinity Domain. Document any policies regarding the provision of liability insurance for those publishing documents to, or using documents from, the XDS Affinity Domain.

mm.10-IM.04
Indemnification

Describe how indemnification is dealt with in this XDS Affinity Domain implementation. To give the reader a better idea of what to include in this section, we provide a few guiding scenarios:

mm.10-IM.04
Providers of data create indemnification agreements with all possible users of data.

4.15 Boiler Plate Contract Provisions (BP)

BP.01 Applicable Law

ph.06-BP.01
Governing Law. This Agreement shall be governed by the laws and decisions of the State of [State] and federal privacy laws such as HIPAA, to the extent they preempt [State] state law.

mm.10-BP.01
The U.S. constitutional provision most frequently advanced in a discussion of the states' authority to enter into agreements with foreign sovereigns is found in Article I §10, clause 1. It provides that "[n]o State shall enter into any Treaty, Alliance, or Confederation."[27] Article 1 §10, clause 3 appears to amplify this prohibition: "No State shall, without the Consent of the Congress . . . enter into any Agreement or Compact with another State, or with a foreign Power."[28] The framers may have drawn some distinction between the "treaty, alliance, or confederation" of the 1st clause and the "agreement or compact" of the 3rd clause. However, the distinction – if any – is not explored in this briefing paper.

These two provisions work to ensure the supremacy of the government of the United States in the field of foreign relations. The federal government's power in this field arises both from express and implied grants of authority by the U.S. Constitution. Article II §2, clause 2 expressly gives the President "Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur."[29] This power is not limited to entering into formal Treaties but has been held to extend to entering into and enforcing other kinds of international agreements falling short of treaties.[30] The Supreme Court has stated that this authority derives not from the U.S. constitution but, instead, is inherent in the federal government's position as a sovereign international power.[31]

mm.10-BP-01
Relatively few judicial opinions interpret the effect of Article I on the states' power to enter into agreements. In many areas of legal research this might be taken as an indication that the applicable law in a particular area is both well settled and little-used. State and federal case law examining the question of state competence to enter into international agreements favors a very high degree of protection for the federal government's power to control the conduct of foreign affairs and to preclude state interference with external relations. An excellent overview of this is provided by the United States Court of Appeals for the First Circuit in National Foreign Trade Council v. Natsios, 181 F.3d 38 (1st Circ. 1999). See also Crosby v. National Foreign Trade Council, 530 U.S. 363 (2000).

[27] USCA Const. Art. I §10, cl. 1.
[28] USCA Const. Art. I §10, cl. 3.
[29] USCA Const. Art. II §2, cl. 2.
[30] 16A Am Jur 2d, Constitutional Law §234, citing B. Altman & Co. v. U.S., 224 U.S. 583, 32 S.Ct. 593, 56 L. Ed. 894 (1912).
[31] U.S. v. Curtiss-Wright Export Corporation, 299 U.S. 304, 57 S. Ct. 216, 81 L. Ed. 255 (1936).

More briefly, the U.S. Supreme Court stated the principle of broad federal supremacy over external matters in United States v. Pink, holding that "[p]ower over external affairs is not shared by the States; it is vested in the national government exclusively"[32]; the Court has emphasized the "oneness" of our nation with respect to transactions with foreign nations[33] and that federal power over foreign relations should "be left entirely free from local interference."[34] The Court in Zschernig v. Miller, for example, determined that a state's detailed inquiries into the judicial processes and policies of a foreign sovereign affected international relations and could adversely affect the federal government's ability to manage international affairs even in the absence of a treaty.[35]

mm.10-BP.01
Legal Governance

Define policies regarding the governance of legal issues related to users, publishers, IT staff, and vendors involved in the XDS Affinity Domain or within XDS Affinity Domains of the region or nation for which these policies are defined.

mm.09-BP.01
3. Legal Framework

The following section reviews the legal framework currently in place for implementing these guidelines, from the perspective of the US federal and state governments and the government of Mexico.

Federal and State Governments of the United States

mm.09-BP.01
The Public Health Service Act (42 USC § 241 et seq) provides the Department of Health and Human Services (HHS) with a broad authority to conduct activities relating to the prevention and control of diseases and injuries. It also authorizes HHS to participate with other countries in cooperative endeavors to advance health sciences and improve the health of Americans. Requirements for disease reporting are typically defined in laws at the state and local level. The Centers for Disease Control and Prevention (CDC), however, together with the Council of State and Territorial Epidemiologists (CSTE) have defined a national list of notifiable diseases, and states provide information on these diseases to CDC's National Notifiable Diseases Surveillance System. In addition, ships and airlines are required by federal regulation to report deaths or ill passengers to CDC quarantine stations.

mm.09-BP.01
CDC also operates various surveillance systems that track particular disease problems of national interest. The Privacy Act (5 USC § 552a) regulates certain terms of use by federal agencies of "systems of records" which include personal identifying information, as might apply to surveillance databases. While the Act sets controls on the terms by which federal agencies can gather, maintain, disseminate personal information, it also defines circumstances in which disclosure of information is permissible without the subject's consent. This includes disclosure "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual" and pursuant to a routine use as defined in the system of records published by the agency. The system of records applicable to most of CDC's surveillance projects, "Epidemiologic Studies and Surveillance of

[32] U.S. v. Pink, 315 U.S. 203,233, 62 S.Ct. 552, 86 L. Ed. 796 (1942).
[33] Chae Chan Ping v. United States, 130 U.S. 581, 606, 9 S.Ct. 623, 32 L. Ed. 1068 (1889).
[34] Hines v. Davidowitz, 312 U.S. 52, 63, 61 S.Ct. 399, 85 L. Ed. 581 (1941).
[35] Zschernig v. Miller, 389 U.S. 429, 441, 88 S.Ct. 664, 19 L. Ed. 683 (1968).

Disease Problems" authorizes, among other things, disclosure to "cooperating medical authorities."

mm.09-BP.01
The Freedom of Information Act (FOIA, 5 USC § 552) allows persons to request access to federal agency records. It applies only to federal records, though US states have their own equivalent statutes. The FOIA provides access to all federal agency records except for those records (or portions of records) that are protected from disclosure. While FOIA protects certain classes of information from disclosure, it would not appear to restrict the sharing of public health information with counterparts in Mexico as described in this document.

mm.09-BP.01
Each state must review its laws relating to these guidelines to determine whether legal authority exists to exchange public health information and to collaborate in other ways with counterparts in Mexico on epidemiologic issues of mutual interest. Some states have examined their legislation, seeking to identify potential barriers to the sharing of epidemiologic information with Mexico.[36,37]All states are encouraged to complete an analysis of their laws for this purpose. In those cases where barriers are identified, states are encouraged to consider new legislation that would provide such authority, based on the value of such collaboration for the improvement of public health in our countries.

mm.09-BP.01
The US Constitution, Article I, section 10, states in relevant part that "No state shall, without the consent of Congress, enter into any agreement or compact with another state, or with a foreign power..." With the approval of the State Department, however, states have the ability to enter into "non-binding" cooperative arrangements with each other and with their Mexican counterparts. Current plans to share epidemiologic information should be able to proceed under such arrangements.

mm.09-BP.01
In summary, US federal legislation permits the sharing of epidemiologic information with a foreign country for the prevention or control of disease, with necessary restrictions based on confidentiality. Each state needs to review its own legislation to determine whether barriers exist to the exchange of such information. If present, this legislation should be reconsidered to ensure that state public health officials have the needed authority to improve the public's health through the sharing of such information. With the requisite authority under state law, states would be constitutionally permitted to enter into cooperative arrangements with each other and with Mexican states for the purpose of sharing epidemiologic information.

mm.09-BP.01
Government of Mexico

The legal framework of Mexico for epidemiologic surveillance is defined by an extensive set of determinations which include the Mexican Constitution, laws, regulations, decrees, agreements, norms, and decisions of the National Epidemiologic Surveillance Council (Annex 1). These legal instruments, created by or with the collaboration of the Secretaria de Salud, (SSA) indicate the steps to be taken to notify epidemiologic events within the country as

[36] Barriers to Binational Cooperation in Public Health between Texas and Mexico, Office of Border Health, Texas Department of Health, 2001.

[37] Annual Border Health Status Report, 2001: Barriers to California-Mexico Collaboration in Public Health, California Office of Binational Border Health, California Department of Health Services.

well as the procedures to share such information with other countries ruled by the International Health Regulations.

mm.09-BP.01
Other US-Mexico Collaborations

HHS and SSA have established Memoranda of Cooperation in health and in epidemiology, respectively. The first defined one of the areas of cooperation as being "Health and human information systems, including telecommunications, statistical methodologies, and information exchange." The second specified the activities to include "Development and implementation of protocols in support of epidemiological surveillance which are of mutual interest" and exchange of resources, including "jointly acquired public health information."

mm.09-BP.01
In 2000 the US and Mexico signed an agreement creating the US-Mexico Border Health Commission. Among the functions to be carried out by the Commission is "to conduct or support a binational, public-private effort to establish a comprehensive and coordinated system, which uses advanced technologies to the maximum extent possible, for gathering health-related data and monitoring health problems in the United States -Mexico Border Area." The agreement contemplates significant state involvement in the Commission's activities, requiring that the health officers from each of the ten border states be appointed as Commission members, together with 12 other representatives from the border states of each country.

mm.09-BP.01
Other existing mechanisms for collaboration between governments of the two countries on public health issues include the US-Mexico Binational Commission, the US-Mexico Food Safety Cooperative Agreement, the Border Governor's Conference, the Pan American Health Organization (PAHO) El Paso Field Office, border state Memoranda of Understanding, and Binational Health Councils of border Sister Cities. Joint public health collaborations are in place between the two countries in the areas of tuberculosis (Ten Against TB, Binational TB Card), infectious disease surveillance (Border Infectious Disease Surveillance—BIDS, Early Warning Infectious Disease Surveillance—EWIDS), and others.

mm.09-BP.01
In conclusion, the legal frameworks of the two countries at the national level allow for the exchange of information, as proposed in these guidelines. States will need to determine how their legislation relates to the Guidelines provided here. Numerous interfaces are already in place between health authorities of the US and Mexico, reflecting the need and desire to assist each other in confronting shared public health challenges.

mm.09-BP.01
At the national level within the United States, the CDC is responsible for surveillance of human illness caused by foodborne disease and for epidemiological and laboratory investigation of outbreaks of foodborne illness. The United States Department of Agriculture (USDA) is responsible for regulating meat, poultry, and processed egg products. The Food and Drug Administration (FDA) is responsible for regulating all other foods, which includes seafood, dairy fruits, vegetables, and shell eggs, among other products.

mm.09-BP.01
At the state level in the US, the foodborne illness surveillance and investigation responsibility rests with the health agency at the state and local level, while the regulatory responsibility may rest with the agriculture department or the health department at the

state level or the local health agency at the local level. When states want assistance from the CDC for foodborne outbreak investigations, state officials must make a formal request to CDC since CDC does not have the authority to send investigators without an invitation from state officials. In the event of an inter-state or international foodborne outbreak, the FDA and/or USDA would be contacted in order to cooperate with multiple jurisdictions in coordinating the outbreak investigation, including traceback, trace-forward and potential product recall.

mm.09-BP.01
At the local government level in the US, there is wide variation in food safety roles and responsibilities among the 3,000 local health agencies. In many localities, sanitarians have the primary responsibility for investigating reports of foodborne illness related to food service establishments, whereas in other localities reports of foodborne illness are investigated by state officials and the local sanitarians serve in a secondary support role.

mm.09-BP.01
Within Mexico, as an agency of the Secretaria de Salud, the Federal Commission for Protection against Sanitary Risks (COFEPRIS) is legally responsible for conducting tracebacks of food products associated with foodborne disease. When informed by the United States of a foodborne disease outbreak associated with a product from Mexico, COFEPRIS coordinates internally and externally with other government agencies, according to the nature of the event. COFEPRIS has a Memorandum of Understanding signed with the FDA, as well as with Canadian agencies, for coordination of action in outbreaks of binational interest, to share information, to establish communication contacts and to prepare joint press releases. As part of this trilateral framework procedures for quick and efficient response to address all emergencies are in place to provide protection to the citizens within the three countries.

mm.10-BP-01
However, notwithstanding the federal government's preeminence in the field of foreign relations, the Constitution appears to recognize that the states have a natural interest in matters extending across national boundaries: "No State shall, without the Consent of the Congress . . . enter into any Agreement or Compact with another State, or with a foreign Power" [emphasis added].[38] Some U.S. Supreme Court opinions have been interpreted to suggest that the federal government may acquiesce in a state's encroachment into foreign relations and that the importance of federal preeminence in foreign relations does not always and necessarily preclude state action affecting it.[39] A federal statute or joint resolution expressing Congress' approval that states enter into foreign relations would appear to be a sufficient manifestation of congressional consent to survive constitutional scrutiny – but there is no such statute readily identifiable regarding emergency preparedness.

mm.10-BP-01
Federal legislation does provide that [t]he Director [FEMA] shall give all practicable assistance to States in arranging, through the Department of State, mutual emergency preparedness aid between the States and neighboring countries.[40]

[38] USCA Const. Art. I §10, cl. 3. See also The Restatement (Third) of Foreign Relations Law of the United States §201.

[39] See Barclays Bank PLC v. Franchise Tax Board, 512 U.S. 298, 114 S.Ct. 2268, 129 L. Ed.2d 244 (1994); Wardair Canada Inc. v. Florida Dep't of Revenue, 477 U.S. 1, 106 S.Ct. 2369, 91 L.Ed.2d 1 (1986).

[40] 42 U.S.C. §5196(a) (2003).

In this section Congress speaks to "mutual emergency preparedness aid", not "emergency aid." Arguably "emergency preparedness aid" refers to pre-event planning and resource exchange and, therefore, perhaps to cross-border arrangements.[41] Following this line of reasoning, it suggests Congress' anticipation that states may pursue forms of cooperation across national borders (i.e., "neighboring countries"). Whether or not states must seek the assistance of FEMA under these circumstances is unclear.

Non-binding "commitments" remain the simplest option for cross-border cooperation and may be the most politically expedient choice. As a general matter, states wishing to enter into "non-binding", cross-border emergency preparedness agreements are free to do so. Even for these initiatives, however, the federal government prefers that officials of the Treaty Office of the State Department review the instruments to ensure that they employ non-binding language, do not trigger Constitutional concerns and do not affect other aspects of federal policy.[42]

mm.10-BP-01
CSPS Action-Research Roundtable on Managing Canada-US Relations. Building cross-border links: a compendium of Canada-US government collaboration, Canada School of Public Service (2004).

mm.10-BP.01
Each signatory shall provide copies of their respective statutes or regulations related to public health emergencies and deadly agents to every other signatory. Each signatory shall ensure that the copies so provided are accurate and current. The signatories shall jointly identify and maintain in common a set of materials which they agree reflect the applicable laws and regulations of the Governments of the United States and Canada.

ph.02-BP.01
14. Applicable Law. This Agreement shall be interpreted according to the regulations issued by the United States Department of Health and Human Services pursuant to HIPAA, and the laws of the State of [State Name].

hh.06-BP.01
21.01 Governing law. In the event of a dispute between or among the Participants arising out of this Agreement, the applicable federal and state conflicts of law provisions that govern the operations of the Participants involved in the dispute shall determine governing law.

ss.08-BP.01
Information thus obtained shall not be disclosed, except to individuals expressly authorized to review such information under federal or State laws.

ss.08-BP.01
No records or any information acquired from [State Department] shall be disclosed except as expressly authorized under federal and State law and regulations.

[41] Properly defining "mutual preparedness aid" is essential to the validity of this argument and requires further research.

[42] Compare, 22 CFR §181.4 (Consultations with the Secretary of State), applying to agreements of the United States.

pp.06-BP.01
Section 13.08 Compliance With Laws. The Parties to this Agreement intend and in good faith believe that this Agreement complies with all federal, state, and local laws. If any provision of this Agreement is declared void by a court or arbitrator, or rendered invalid by any law or regulation, that portion shall be severed from this Agreement, and the remaining provisions shall remain in effect, unless the effect of the severance would be to substantially alter the Agreement or obligations of the Parties, in which case, the Parties agree to attempt in good faith to renegotiate the Agreement to comply with such law(s) to the satisfaction of all Parties. In the event the Parties are not able to mutually agree to a new agreement within one hundred eighty (180) days, then this Agreement shall terminate and all data shall be returned to each Participant and the data shall be deleted from the Network.

ph.06-BP.01
Governing Law. This Agreement shall be governed by the laws and decisions of the State of [State] and federal privacy laws such as HIPAA, to the extent they preempt [State] state law.

ph.06-BP.01
16. General Provisions. Miscellaneous provisions that apply to the SNO Terms and Conditions.

16.1 Applicable Law. The interpretation of the Terms and Conditions and the resolution of any disputes arising under the Terms and Conditions and Participants' Registration Agreements shall be governed by the laws of the State of ___________. If any action or other proceeding is brought on or in connection with the Terms and Conditions or a Registration Agreement, the venue of such action shall be exclusively in _____________ County, in the State of ____________.

ss.05-BP.01
In any question that arises pursuant to this Agreement, signatories will be bound by their own local law.

ss.05-BP.01
Nothing in this Agreement is intended to create binding international law.

ss.05-BP.01
This Agreement is subject to the laws of the United States of America, Canada and the several signatories. This Agreement is not to be applied in derogation of any superseding law of the

United States or Canada.

ss.08-BP.01
In addition to the above, the Participants are required to abide by all general requirements contained in Sections IV and V of this Agreement.

(A.) Mandatory General Provisions

ss.08-BP.01
1. During the term of this Agreement, each Participant shall comply with all federal, state and municipal laws, rules and regulations generally applicable to the activities performed pursuant to this Agreement.

BP.02 Venue/Jurisdiction

ss.08-BP.02
The laws of the State of [State] govern this agreement for the [DHSS] participants and the laws of [State] and [City], where applicable, govern this agreement for the [State] participants.

pp.06-BP.02
Section 13.01 Governing Law. The scope, performance, validity, enforcement, and all other aspects of this Agreement shall be governed by the laws of the State of [State], unless otherwise preempted by the laws of the United States of America.

ss.05-BP.02
A "jurisdiction" is a governmental unit having a territory of control as or in a First Nation, Tribal, state, province or other government unit, including agencies and ministries.

BP.03 Assignability/non-assignability

sp.02-BP.03
8. Assignment.

The [Program] Management Committee and [Entity] may assign this Agreement at their reasonable discretion to a nonprofit corporation, foundation, company, trust, association or other entity established for the specific purpose of administering the [Program] Cardiac Registry, in the event such assignment is deemed desirable for any purpose. The Participant may assign this Agreement to any entity or organization which is his/her/its successor in interest in the provision of health care to individuals whose case information has been submitted to the [Program] Cardiac Registry by or on behalf of the Participant, subject to the reasonable approval of the [Program] Management Committee. In the event of any assignment this Agreement shall bind and shall inure to the benefit of the assignor's successor in interest.

hh.06-BP.03
No party shall assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns.

ph.06-BP.03
16.2 Non-Assignability. No rights of the Participant under its Registration Agreement may be assigned or transferred by the Participant, either voluntarily or by operation of law, without the prior written consent of [SNO Name], which it may withhold in its sole discretion.

ph.06-BP.03
Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. Hospital shall not assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party's obligations under Sections 2 and 6 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such

obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

ph.06-BP.03
Assignment. This agreement shall not be assignable by either party except upon the written consent to such assignment by the other party.

hh.06-BP.03
21.03 Assignment. The Participants shall not assign or transfer this Agreement or any part thereof, without prior review and written consent of all other Participants and ONC, and any such assignment without the Participants' and ONC's written consent shall be void and have no binding effect.

pp.06-BP.03
Section 13.06 Succession and Assignment. This Agreement will be binding on, and will inure to the benefit of, the Parties and their respective successors and assigns. No party may assign or transfer any rights or obligations under this Agreement without the prior written consent of the other Parties, which consent shall not be unreasonably withheld.

ph.06-BP.03
Assignment. This agreement shall not be assignable or transferable by Patient or [State Organization] except upon the written consent to such assignment by the other party.

ph.02-BP.03
17. Assignment. This Agreement may not be assigned, in whole or in part, by RESEARCHER to any third person or entity, without the prior written approval of the Data Provider, which may be withheld at the Data Provider's sole discretion.

BP.04 Third Party Beneficiaries

ss.05-BP.04
This Agreement does not create any right in, or responsibilities to, third parties.

hh.06-BP.04
21.12 Third-Party Beneficiaries. With the exception of (1) the Participants to this Agreement and (2) ONC, there shall exist no right of any Person to claim a beneficial interest in this Agreement or any rights occurring by virtue of this Agreement.

pp.06-BP.04
Section 13.07 No Third Party Rights. This Agreement does not and will not create in any natural person, corporation, partnership, or other organization any benefits or rights, and this Agreement will be effective only as to the Parties and their successors and assigns.

ph.06-BP.04
16.3 Third-Party Beneficiaries. There shall be no third-party beneficiaries of any Registration Agreement.

BP.05 Force Majeure

ph.06-BP.05
16.4 Supervening Circumstances. Neither the Participant nor [SNO Name] shall be deemed in violation of any provision of a Registration Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control. This Section 16.4 (Supervening Circumstances) shall not apply to obligations imposed under applicable laws and regulations or obligations to pay money.

BP.06 Severability

ph.06-BP.06
16.5 Severability. Any provision of the Terms and Conditions or any Participant Registration Agreement that shall prove to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provision of the Terms and Conditions or such Registration Agreement, and such other provisions shall remain in full force and effect.

hh.06-BP.06
21.07 Validity of Provisions. In the event any Section, or any part or portion of any Section of this Agreement, shall be held invalid, void or otherwise unenforceable, each and every remaining section or part or portion thereof shall remain in full force and effect.

ph.02-BP.06
16. Severability. If any portion of this Agreement shall for any reason be invalid or unenforceable, such portions shall be ineffective only to the extent of such invalidity or unenforceability, and the remaining portions shall remain valid and enforceable and in full force and effect.

ph.06-BP.06
Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. Hospital shall not assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party’s obligations under Sections 2 and 6 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

mm.10-BP.06
Severability: In the event that any term or provision of this Agreement shall violate any applicable law, such provision does not invalidate any other provision hereof.

hh.06-BP.06
If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect.

BP.07 Notice

hh.06-BP.07
All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

mm.10-BP.07
Notice: Any notice or other communication required under this Agreement shall be in writing and sent to the address set forth below. Notices shall be given by and to the Manager, [Program], on behalf of [Program], and by and to the designated Contact Person, on behalf of Participating Clinic, or such authorized designee as either party may designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

ph.06-BP.07
Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. Hospital shall not assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party’s obligations under Sections 2 and 6 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

pp.06-BP.07
Section 13.09 Notice. All notices, requests, demands, and other communications associated with this Agreement shall be in writing and will be deemed to have been duly given on the date of service if served personally on, or by facsimile transmission to, the party to whom notice is to be given, or on the third day after mailing if mailed to the party to whom notice

is to be given by certified mail, return receipt requested, and properly addressed to the individuals executing this Agreement on behalf of the respective Parties as set forth on the signature portion of this Agreement, with a copy to other persons as such Parties may designate in writing to [Organization].

pp.06-BP.07
Section 13.12 Notification of Claims. Each Party shall promptly notify all other Parties upon notification or receipt of any civil or criminal claims, demands, causes of action, lawsuits, or governmental enforcement actions arising out of or related to this Agreement, regardless of whether the other Parties are named as a party in such claims, demands, causes of action, lawsuits, or enforcement actions.

pp.06-BP.07
Section 13.13 Regulatory References. A reference in this Agreement to a section in a federal, state, or local statute, law, or regulation means the section as in effect or as amended.

ph.02-BP.07
18. Notices. Any notices made in connection with this Agreement shall be in writing and sent certified mail, to the following addresses:

ph.06-BP.07
d. Notice. All notices and other communications required or permitted to be given shall be made in writing and shall be considered given and received when (a) personally delivered to the other party; (b) delivered by courier; (c) delivered by facsimile; or (d) deposited in the US. Mail, postage prepaid, return receipt requested and addressed as set forth below or at such other address such party shall have specified by notice given in accordance with the provisions of this section.

ph.06-BP.07
Notice. All notices and other communications required or permitted to be given shall be made in writing and shall be considered given and received when (a) personally delivered to the other party; (b) delivered by courier; (c) delivered by facsimile; or (d) deposited in the U.S. Mail, postage prepaid, return receipt requested and addressed as set forth below or at such other address such party shall have specified by notice given in accordance with the provisions of this section.

ph.06-BP.07
15.2.3 Rules for Indemnification.

Provisions governing the parties' indemnification obligations. Any indemnification made pursuant to the Terms and Conditions shall include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys' fees and any settlement by or judgment against the party to be indemnified. In the event that a lawsuit is brought against the party to be indemnified, the party responsible to indemnify that party shall, at its sole cost and expense, defend the party to be indemnified, if the party to be indemnified demands indemnification by written notice given to the indemnifying party within a period of time wherein the indemnifying party is not prejudiced by lack of notice. Upon receipt of such notice, the indemnifying party shall have control of such litigation but may not settle such litigation without the express consent of the party to be indemnified, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third parties, be a waiver of any defense or immunity otherwise available, and the indemnifying party, in indemnifying the indemnified party, shall be entitled to assert in any action every defense or immunity that the indemnified party could assert on its own behalf.

ph.06-BP.07
4.5 Changes to Terms and Conditions. How Participants will be aware of changes to the SNO Terms and Conditions, and will be legally obligated to comply therewith. [SNO Name] may amend, repeal and replace the Terms and Conditions at any time, and shall give Participants notice of those changes, as described in Section 3.2 (Development and Dissemination; Amendments). Subject to Section 4.6 (Termination Based on Objection to Change), any such change to the Terms and Conditions shall automatically be incorporated by reference into each Registration Agreement, and be legally binding upon [SNO Name] and the Participant, as of the effective date of the change.

hh.06-BP.07
20. Notices. All notices to be made under this Agreement shall be given in writing to the appropriate Participant’s representative at the address listed on Attachment 4, and shall be deemed given (i) upon receipt, if delivered in person or sent by facsimile transmission if the sending facsimile machine receives confirmation of receipt by the receiving facsimile machine, or (ii) within three days after deposit in the United States mail, if sent certified mail, return receipt requested.

21. Miscellaneous/General.

ph.06-BP.07
16.6 Notices. Any and all notices required or permitted under the Terms and Conditions shall be sent by United States mail, overnight delivery service, or facsimile transmission to the address provided by the Participant in its Registration Form or such different addresses as a party may designate in writing. If the Participant has supplied [SNO Name] with an electronic mail address, [SNO Name] may give notice by email message addressed to such address; provided that if [SNO Name] receives notice that the email message was not delivered, it shall give the notice by United States mail, overnight delivery service, or facsimile.

ph.06-BP.07
4. Changes to Terms and Conditions

The [SNO Name] Terms and Conditions shall be subject to change from time to time, and all such changes shall be incorporated by reference into this [Participant] Registration Agreement upon the effective date selected by [SNO Name]. The [Participant] shall be informed of all such changes prior to their effectiveness. If the [Participant] objects to the changes, the [Participant] may terminate this Agreement and, by doing so, cease to be a [Participant], as described in the [SNO Name] Terms and Conditions.

BP.08 Waiver

ph.06-BP.08
16.7 Waiver. No provision of the Terms and Conditions or any Participant Registration Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of a breach by the other, whether expressed or implied, shall not constitute a consent to, waiver of, or excuse for any other different or subsequent breach.

pp.06-BP.08
Section 13.16 Waiver of Breach. No failure or delay by any party in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any breach shall constitute a waiver of any prior, concurrent, or subsequent breach.

ph.06-BP.08
15.2.3 Rules for Indemnification.

Provisions governing the parties' indemnification obligations.

Any indemnification made pursuant to the Terms and Conditions shall include payment of all costs associated with defending the claim or cause of action involved, whether or not such claims or causes of action are meritorious, including reasonable attorneys' fees and any settlement by or judgment against the party to be indemnified. In the event that a lawsuit is brought against the party to be indemnified, the party responsible to indemnify that party shall, at its sole cost and expense, defend the party to be indemnified, if the party to be indemnified demands indemnification by written notice given to the indemnifying party within a period of time wherein the indemnifying party is not prejudiced by lack of notice. Upon receipt of such notice, the indemnifying party shall have control of such litigation but may not settle such litigation without the express consent of the party to be indemnified, which consent shall not be unreasonably withheld, conditioned or delayed. The indemnification obligations of the parties shall not, as to third parties, be a waiver of any defense or immunity otherwise available, and the indemnifying party, in indemnifying the indemnified party, shall be entitled to assert in any action every defense or immunity that the indemnified party could assert on its own behalf.

ph.06-BP.08
Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. Hospital shall not assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party's obligations under Sections 2 and 6 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

hh.06-BP.08
21.05 Waiver. Participant's failure to insist on performance of any term, condition, or instruction, or to exercise any right or privilege included in this Agreement, or its waiver of any breach, shall not thereafter waive any such term, condition, instruction, and/or any right or privilege.

ss.08-BP.08
3. Failure by any of the Participants to exercise any right or demand performance of any obligation under this Agreement shall not be deemed a waiver of such right or obligation.

hh.06-BP.08
No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof.

BP.09 Breach

sp.08-BP.09
Clinic is responsible for appropriately using the [State IIS] software for the sole purpose of participating in [State IIS]. The [State IIS] purpose is to maintain a database of all children immunized at Clinic and in [State] with a goal of age-appropriate immunizations. Other uses of [State IIS] are inappropriate and forbidden. Inappropriate uses of the software include, but are not limited to, assisting in bill collection or locating or identifying persons for reasons other than increasing immunization levels. Inappropriate uses may result in Clinic's exclusion from the [State IIS], as well as other civil or criminal penalties.

ph.06-BP.09
Miscellaneous. This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement. This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties. No failure or delay by either party in exercising any right hereunder will operate as a waiver thereof. Hospital shall not assign this Agreement, or any of the rights or obligations contained herein. This Agreement shall be binding on the parties, their successors and permitted assigns. The parties agree that any breach of a party's obligations under Sections 2 and 6 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction. If any provision of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remaining portions shall remain in full force and effect. All notices required under this Agreement shall be: (a) in writing; and (b) deemed to have been duly made and received when (i) personally served, (ii) delivered by commercially established courier service, or (iii) ten (10) days after deposit in the mail via certified mail, return receipt requested, to the addresses specified in the first paragraph of this Agreement or to such other address as the parties shall designate in writing from time to time.

BP.10 Miscellaneous Boilerplate Provisions

mm.10-BP.10
Supersession: This Agreement contains the entire agreement between the parties. All other prior discussions, communications, and representations concerning the subject matter of this Agreement are superseded by the terms of this Agreement**.**

mm.10-BP.10
Intellectual Property Rights to Published Documents

Define how intellectual property rights will be managed for documents published to the XDS Affinity Domain. For example, define whether property rights are maintained in any way once documents are published or if they are immediately waived.

Amendment: This Agreement may be amended only in writing signed by both parties and each amendment shall be attached to and become a part of this Agreement.

pp.06-BP.10
Section 10.01 Composition and Duties of Management Committee. Each Participant will be entitled to be represented by two individuals on a Management Committee to coordinate the operations of the Network and to have full authority to act on behalf of the Participant with regard to Network operations. [Organization] shall also be represented by two individuals on the Committee, however [Organization] may have any number of observers on the Committee to help accomplish the work of the Committee. Each Party shall specifically identify their Management Committee representatives in writing to [Organization]. Communications and notices regarding the Network shall be provided to the named representatives and [Organization] shall be able to fully rely on the actions and representations of a Participant's designated representatives or any proxy representative that the Participant chooses to send to a meeting or communicate with [Organization], and shall be fully protected in such reliance. This Committee will meet from time to time, but not without at least seven days’ notice, to consider and resolve various issues surrounding the Network, including, but not limited to: technical issues, confidentiality, the scope of Information stored and accessed by Participants, the use of the Information, and any other issues related to the Network or the Participants’ participation therein.

pp.06-BP.10
Section 10.02 Voting. Each Participant and [Organization] shall be entitled to exercise one vote on decisions made by the Committee, regardless of the number of their respective Committee members. At any meeting of the Management Committee, the holders of a majority of the eligible votes that may be voted on the business to be transacted at such meeting shall constitute a quorum, and a vote of 80% of the votes held by the members of the Committee constituting the quorum shall be necessary for the transaction of any business at the meeting. No decision made by the Management Committee may contravene any provision of the Agreement or the spirit or intent thereof.

pp.06-BP.10
Section 10.03 Force of Management Committee Decisions. Any decisions made by the Management Committee in accordance with Section 10.02 shall control the relationship between the Parties and their respective obligations hereunder, and shall be binding on all Parties notwithstanding any other provision of this Agreement unless: (a) a specific Section of this Agreement affirmatively prevents its alteration by the Management Committee; or (b) a Party objects in writing (i) within ten (10) days after a Management Committee decision is made with which it objects, or (ii) in the case of a meeting at which the Party’s representatives were not present, within ten (10) days after receipt of written notification of the Management Committee decision. Such an objecting Party shall be entitled to abstain from complying with such decision without penalty unless the Party’s concerns regarding the decision are accommodated by the other Parties to this Agreement.

pp.06-BP.10
Section 11.01 Amendment. This Agreement contains the entire agreement of the Parties and supersedes all previous negotiations and agreements, whether written or oral, including, but not limited to the First Agreement. This Agreement may be amended only by an instrument

in writing signed by the Party against whom the change, waiver, modification, extension, or discharge is sought, unless otherwise indicated in this Agreement.

pp.06-BP.10
Section 11.02 Addition of New Participants. The Participants acknowledge that additional Participants may be added to the Network. Such additional Participants may be added to the Network upon approval of the Management Committee in compliance with Section 10.02. Subsequent Participants shall be required to execute an Agreement substantially similar to this Agreement.

pp.06-BP.10
Section 13.02 Multiple Counterparts. This Agreement may be executed in multiple counterparts, each of which will be deemed an original, but all of which together will constitute one and the same

pp.06-BP.10
Section 13.03 Incorporation By Reference. All exhibits attached to this Agreement are incorporated by reference and made a part of this Agreement as if those exhibits were set forth at length in the text of this Agreement.

pp.06-BP.10
Section 13.04 Gender. Any reference to gender will be deemed to include the masculine, the feminine, and the neuter genders unless the context otherwise requires.

pp.06-BP.10
Section 13.05 Headings. Any subject headings used this Agreement are included for purposes of convenience only, and shall not affect the construction or interpretation of any of its provisions.

pp.06-BP.10
Section 13.10 Independent Contractors. It is mutually understood and agreed that in performing their respective duties and obligations hereunder, the Parties are at all times acting as independent contractors with respect to each other. Nothing in this Agreement shall constitute or be construed to create a partnership or joint venture between or among the Parties.

pp.06-BP.10
Section 13.11 Conditional Participation. Each Participant’s participation in the Network is conditional on the continued control and development of the repository software by [Organization] and the operation and management of the Network by [Organization] or its subcontractor. This Agreement shall be voidable and the Participants shall be entitled to withdraw pursuant to Section 12.03 of this Agreement if another party acquires control of the Network.

pp.06-BP.10
Section 13.14 Ethical and Religious Directives. The Parties acknowledge that the operation of [Hospital] and [Health Center] and their participation in the Network in accordance with the [Entity] Directives are matters of conscience. It is the intent and agreement of the Parties that neither this Agreement nor any part hereof shall be construed to require [Hospital] or [Health Center] to violate said Directives in their operation and all parts of this Agreement must be interpreted in a manner that is consistent with said Directives.

pp.06-BP.10
Section 13.15 Corporate Compliance. The Parties acknowledge that some or all of them have in place a Corporate Compliance Program ("Program") which has as its goal to ensure that the Party complies with federal, state, and local laws and regulations. These Programs focus on risk management, the promotion of good corporate citizenship, including the commitment to uphold a high standard of ethical and legal business practices, and the prevention of misconduct. The Parties acknowledge one another's respective commitments to their Programs and agree to conduct all business transactions which occur pursuant to this Agreement in accordance with the underlying philosophy of Program Compliance adopted by the respective Parties.

ph.02-BP.10
12. Relationship Between Parties. Nothing contained in this Agreement shall constitute or be construed to create, a partnership, joint venture, agency or any other relationship besides that of independent parties to this Agreement.

ph.02-BP.10
15. Entire Agreement. This Agreement supersedes any and all other agreements, either oral or in writing, between the parties with respect to the use and disclosure of limited data sets for purposes of research testing BIOSURVEILLANCE, and contains all of the covenants and agreements between them with respect to that activity. Each party acknowledges that no representation, inducement, promise or agreement, orally or otherwise, has been made by any party, or anyone acting on behalf of any party, which is not embodied within this Agreement. Any modifications to this Agreement shall be effective only if in writing and signed by the other party.

ph.06-BP.10
The Terms and Conditions, and Policies and Procedures, shall be subject to change from time to time, and all such changes shall be incorporated by reference into this Registration Agreement upon the effective date selected by [RHIO]. Participant shall be informed of all such changes prior to their effective date. If Participant objects to the changes, the Participant may (a) terminate this Agreement, or (b) may petition [RHIO] for reconsideration, pursuant to the Terms and Conditions and if dissatisfied with the results may terminate this Agreement. By terminating this Agreement, Participant shall cease to be a participant in [RHIO], and shall no longer have access to the System or the Services, all as more fully set forth in the Terms and Conditions and the Policies and Procedures.

ph.06-BP.10
The parties to this Agreement acknowledge that it may be necessary or desirable to amend the Terms and Conditions, prior to the Go Live Date, and shall use their respective best efforts with each other, and with the other Hospital Type participants that have executed Registration Agreements with [RHIO] during the Initial Registration Period, to reach agreement as to such amendments during the Interim Registration Period so as to avoid a gap in services from [RHIO] and to permit this Agreement to continue beyond the Initial Registration Period.

ph.06-BP.10
Entire Agreement. This Agreement constitutes the entire agreement between Patient and [State Organization] with respect to access to the Network.

ph.06-BP.10
None of the provisions of this Agreement are intended to create any relationship between the parties other than that of independent entities contracting with each other solely for the

purpose of effecting the provisions of this Agreement. Neither of the parties, nor any of their respective officers, directors, employees or agents, shall have the authority to bind the other or shall be deemed or construed to be the agent, employee or representative of the other except as may be specifically provided herein. Neither party, nor any of their employees or agents, shall have any claim under this Agreement or otherwise against the other party for Social Security benefits, workers' compensation, disability benefits, unemployment insurance, vacation, sick pay or any other employee benefits of any kind.

ph.06-BP.10
Entire Agreement. This Agreement constitutes the entire agreement between the parties with respect to access to the Network.

ph.06-BP.10
16.8 Complete Understanding. With respect to any Participant Registration Agreement made pursuant to the Terms and Conditions, that Agreement and the Terms and Conditions together contain the entire understanding of the parties, and there are no other written or oral understandings or promises between the parties with respect to the subject matter of any Registration Agreement other than those contained or referenced in that Registration Agreement. All modifications or amendments to any Registration Agreement shall be in writing and signed by all parties.

SP.06-BP.10
This Agreement addresses the conditions under which CMS will disclose and the User will obtain and use the CMS data file(s) specified in section 7. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the files specified in section 7 and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services or any of its components with respect to the data specified herein. Further, the terms of this Agreement can be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS point-of-contact specified in section 5 or the CMS signatory to this Agreement shown in section 22.

ss.05-BP.10
Nothing in this Agreement is to be construed as an encroachment on the full and free exennise of U.S. federal authority, as an interference with the just supremacy of the U.S, over its several states, as affecting the federal structure of the United States or as enhancing the political power of the party states at the expense of each other or other U.S. states.

SP.06-BP.10
The parties mutually agree that the following specified Attachments are part of this Agreement:

hh.06-BP.10
This Agreement sets forth the entire agreement between the parties and supersedes any and all prior agreements or representations, written or oral, of the parties with respect to the subject matter of this Agreement.

hh.06-BP.10
This Agreement may not be modified, altered, or amended except by a written instrument duly executed by both parties.

hh.06-BP.10
The parties agree that any breach of a party's obligations under Sections 2 and 5 will result in irreparable injury to the other party for which there is no adequate remedy at law. Therefore, in the event of any breach or threatened breach of such obligations, the nonbreaching party will be entitled to seek equitable relief in addition to its other available legal remedies in a court of competent jurisdiction.

sp.08-BP.10
The undersigned has read, understands and agrees to abide by this [Immunization] Registry Security and Confidentiality Agreement and understands other participating providers will have access to data entered into the [Immunization] Registry as outlined within this document.

hh.06-BP.10
21.02 Amendment. No waiver, modification, or amendment to the terms of this Agreement shall be effective unless made in writing and signed by duly authorized representatives of all Participants to this Agreement.

hh.06-BP.10
21.06 Integration. This Agreement sets forth the entire and only Agreement between the Participants relative to the subject matter hereof. Any representations, promise, or condition, whether oral or written, not incorporated herein shall not be binding upon any Participant.

hh.06-BP.10
21.08 Priority. Except with respect to the Prime Contract, in the event of any conflict or inconsistency between a provision in the body of this Agreement and any Attachment hereto, the terms contained in the body of this Agreement will prevail.

hh.06-BP.10
21.09 Headings. The headings throughout this Agreement are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify or aid in the interpretation or construction of meaning of the provisions of this Agreement. All references in this instrument to designated "Sections" and other subdivisions are to the designated Sections and other subdivisions of this Agreement. The words "herein," "hereof" and "hereunder" and other words of similar import refer to this Agreement as a whole and not to any particular Section or other subdivision.

hh.06-BP.10
21.11 Counterparts. This Agreement will become binding when any one or more counterparts hereof, individually or taken together, bears the signatures each of the Participants hereto. This Agreement may be executed in any number of counterparts, each of which will be deemed an original as against the Participant whose signature appears thereon, but all of which taken together will constitute but one and the same instrument.

sp.08-BP.10
Neither Clinic nor any employee or agent thereof will hold him or herself out as, or claim to be, an officer or employee of State and will not make any claim, demand or application to or for any right or privilege applicable to an officer or employee of State including, but not

limited to, workers' compensation, health, life or malpractice insurance, retirement membership or credit, and clinic agrees to assume responsibility for such liabilities.

ss.08-BP.10
4. All data, technical information, materials gathered, originated, developed, prepared, used or obtained in the performance of the requested pilot test, including but not limited to, all papers, reports, surveys, plans, charts, records, analyses or publications produced for or as a result of this Agreement shall bear an acknowledgment of the Participant who provide the data. No work product produced utilizing data obtained under this Agreement shall be released to the public without the prior written consent of the affected Participant. The Participants shall have the right to edit each party's own work product and shall further have the right to add co-authorship or disclaimers as it, in its sole discretion, deems appropriate. The Participants shall assume all responsibilities relative to determining compliance and effect of the [State] Open Public Records Act and as it pertains to work product provided by the Participant.

5. The Participants agree that the information and or service deliverables indicated in Section II (A.)3 will be performed during the period beginning [Date] and the period ending [Date].

ss.08-BP.10
2. Each of the participants is an independent entity and neither party shall hold itself out as an agent, partner or representative of the other.

ss.08-BP.10
If any of the provisions of this Agreement are, or become invalid, to any extent, the other provisions of this Agreement shall not be affected thereby. In the event of the invalidity of a provision, the Participants agree to accept a provision which reflects as closely as possible the intention of the invalid provision.

ss.08-BP.10
This agreement may be modified with express written consent of the Participants.

ss.08-BP.10
MOA extensions may be made to this agreement. If allowed, approval may be granted by the Program Management Officer and the Chief Information Officer.

ss.08-BP.10
Modifications to Section III regarding deliverables to be performed under Section II. (A.)3 may be made with the approval of the Program Management Officer and the Chief Technology Officer identified in Section VI.

sp.06-BP.10
By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement for protection of the data file(s) specified in section 7, and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.