March 31, 2009

Health Information Security and Privacy Collaboration

Adoption of Standard Policies Collaborative Final Report

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

Adoption of Standard Policies Collaborative
Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, Washington

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

Adoption of Standard Policies Collaborative Final Report

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

Adoption of Standard Policies Collaborative
Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, Washington

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

EXECUTIVE SUMMARY

During the first phase of the Health Information Security and Privacy Collaboration (HISPC), one of the major challenges identified to facilitate electronic exchange of health information was mistrust due to variations in privacy and security policies. The critical question was how an organization would determine if its exchange partners used appropriate measures to safeguard electronic health information. To establish a chain of trust, security policies needed to be specified for use in the legal agreements that would support nationwide health information exchange (HIE). The Adoption of Standard Policies Collaborative (ASPC) was formed to develop an approach and process to identify and reconcile the variations in implementation of organizational security policies in health information organizations (HIOs) participating in the HIE process.

ASPC is one of seven multistate collaborative privacy and security projects supported and funded during Phase III of the Health Information Security and Privacy Collaboration (HISPC). The states that participated in the collaborative were Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, and Washington. Each state was authorized by their governor's office, and had the approval of the state government to participate in the collaborative.

ASPC's goal was to define standard policies to achieve interoperability in HIE on multiple organizational levels including statewide HIOs, state and regional HIOs, and HIOs across state boundaries. To determine the parameters that would be included in a policy, the method the collaborative selected was the use case approach. The use case approach is used in software and systems engineering to describe a system's behavior as it responds to requests that originate from the outside. The use case approach uses scenarios to establish the functional requirements. To conduct the use case analysis or mapping, the ASPC selected several state HIOs to determine minimum policy requirements for authentication and audit by using the Harmonized Use Case for Electronic Health Records (Laboratory Results Reporting) and the Medication Management Detailed Use Case developed by the American Health Information Community (AHIC).

Ideally, an omnibus security policy would include proposed requirements for authorization, authentication, access, and audit. Authorization, authentication, access, and audit are all interdependent. A shortened project timeline necessitated a narrower focus. ASPC limited the scope to critical aspects of authentication and audit for providers accessing protected health information through an HIE. Authentication was determined to be critical because it is the cornerstone of privacy and security. Audit was selected because it provides the foundation for accountability and trust, has legal requirements, and carries interdependent value for authorization and access. Consideration of authorization and access were deferred for later analysis.

To define minimum policies for authentication and audit, ASPC developed an approach and process to identity and reconcile variations in differing security policies among the collaborating states. At a high level, this approach comprised an environmental scan of existing best practices for authentication and audit policies and procedures, including:

- review of literature and standards for authentication and audit concepts,
- design of a standard set of questions to determine existing policy within each collaborative state for authentication and audit, and
- development of security policy templates for authentication and audit, use case documentation and analysis.

This approach also encompassed a negotiation of requirements for authentication and audit and policy development that included:

- comparison of each state's use case mapping, articulating similarities and arbitrating differences,
- development of the Uniform Security Policy,
- legal review of the Uniform Security Policy,
- stakeholder outreach, and
- development of the Guide to Adoption of Uniform Security Policy.

ASPC planned to replicate this approach when they evaluated policy needs for authorization and access to protected health information.

Products that ASPC authored include the following publications:[1]

- Uniform Security Policy (USP) and
- The Guide to Adoption of Uniform Security Policy.

The first document defines the minimum policy requirements for authentication and audit for providers accessing protected health information through HIE for treatment purposes. The Guide to Adoption of Uniform Security Policy outlines a process to define and harmonize minimum policy requirements with a focus on authentication and audit. The Guide defines processes and products that must be addressed to achieve consensus on privacy and security policies and practices to support the exchange of electronic health information. This document articulates a stepwise progression to comprehensive policy development as the foundation for secure HIE.

[1] The *Uniform Security Policy* is included as Appendix G and contains the actual policies developed and vetted by the ASPC. The *Guide to Adoption of Uniform Security Policy* is available as a separate publication.

1. INTRODUCTION

1.1 Need for Standard Policies and Procedures

The challenges to ubiquitous electronic health information exchange (HIE) in the United States are well documented. Many states have undertaken a variety of initiatives to foster HIE and the variability in these solutions is the only consistency. The business needs that are the driving HIE, the proposed functions, the organizational structures of the health information organizations (HIOs), the exchange mechanisms, and system architectures are generally unique to each circumstance. This variability creates challenges to interoperability, even within state borders. Efforts to provide a common framework and industry standards have evolved from theoretical discussions to implementation with the Nationwide Health Information Network (NHIN) Trial Implementation. The greatest challenge in this work is not technical, but focuses on establishing the chain of trust. The Adoption of Standard Policies Collaborative (ASPC) set a goal to outline a minimum set of privacy and security parameters that promote intra- and interstate interoperability. An agreed-upon, and adhered-to, minimum set of policy requirements for privacy and security was the best approach to facilitate the sharing of electronic heath records (EHRs). This was a requirement that could be uniquely addressed by an interstate collaborative where members had various approaches to HIE solutions for their states.

The modeling states of Arizona, Colorado, Connecticut, Nebraska, Oklahoma, and Washington either had an HIE infrastructure in operation or were in the process of establishing exchanges. Combining the use case approach with the varied infrastructures and system architectures from such a wide range of states yielded an optimized test environment. ASPC's objective was to develop minimum policy for authentication and audit that would work within any type of infrastructure or architecture and would ensure systems interoperability. Each of the modeling states documented both architecture and business models as a starting point. These data were subsequently used in use case mapping of laboratory results and medication management. The use case mapping provided the basis for the specifying each state's policy requirements based on variations in state law. The modeling states shared and analyzed the set of these policies to negotiate the Uniform Security Policy.

2. THE PROJECT

2.1 Purpose

The purpose of the Adoption of Standard Policies Collaborative (ASPC) was to establish a set of minimum policy requirements, the Uniform Security Policy, for authentication and audit. This policy would forge the first link in the chain of trust among health information organizations (HIOs) to facilitate implementation of ubiquitous interoperable health information exchange (HIE). To support implementation, ASPC developed the Guide to Adoption of Uniform Security Policy. This Guide delineates the process to facilitate policy adoption by other HIOs.

2.2 Scope

The project scope included development of minimum policy requirements for providers accessing protected health information through HIE for treatment purposes. The collaborative recognized that an omnibus security policy would include proposed requirements for authorization, authentication, access, and audit. During the first phases of ASPC's work, priorities for analysis were authentication and audit because the collaborative determined these to be the most critical. Consideration of authorization and access were deferred for later analysis; all four elements, authorization, authentication, access, and audit are interdependent. These minimum policy requirements support authentication and audit for health care providers who access protected health information to benefit and inform treatment. Defining the technical standards for authentication and audit will facilitate interoperability for HIE.

The collaborative focused on two related objectives:

1. To develop a set of minimum policy requirements for authentication and audit referred to as the Uniform Security Policy for providers accessing protected health information through an HIE for treatment purposes.
2. To develop a Guide to Adoption of Uniform Security Policy that will facilitate adoption of the minimum policy requirements by HIOs for HIE.

2.3 Team Members

Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, and Washington participated in the ASPC. Arizona and Connecticut cochaired the group and managed the project timeline, including scheduling meetings, distributing minutes, and attending HISPC Cross-Collaborative Steering Committee meetings. Arizona provided legal counsel. All participating states provided a project director, and most provided additional team members with essential subject matter expertise. The Oklahoma team hosted a SharePoint site that enabled the collaborative to store and share resources and work products throughout the project.

The collaborative's states provided broad representation from the medical stakeholder community, including state government, nonprofits with an interest in HIE, clinicians, hospitals and privacy and security officers. This small and discrete set of stakeholders reviewed the work and helped the collaborative reach consensus within and among states.

2.4 Selection and Documentation of State HIOs in Project Work

Each of the modeling states had HIOs representing widely divergent health information exchange platforms. These platforms were classified into the following categories:

Central Repository: Features a health record that is stored at the HIO's central location. The record is sent to the central location from edge systems contributing patient data. The patient's record is identified by a unique identifier that may be assigned by the central repository. The local record may be a detailed record and the shared record a summary record.

Federated model: Features health records stored at the originating provider. The patient's unified record is delivered by a query and response from different systems and typically uses patient indexes and record locator services. The parameters of the search usually included an agreed-upon subset of data in the point-of-care systems.

Hybrid model: Features a combination of the two architecture types above. Patient records are identified by a combination of identifiers—regional and local—and the central record contains only demographics and limited clinical data with access control and record locators for detailed data.

Banking model: Features a Health Record Banking (HRB) system that emulates the commercial banking industry by using health-record banks to serve the need for immediately accessible and secure data for a diverse variety of stakeholders. The objectives of the HRB are uninterrupted access to patient records, maintenance of the rights of the consumer to control his/her personal health data, and provision of a means for storing all EHRs and data in fail-safe, readily-accessible, secure, and restricted repositories.

All four data exchange architectures described above were represented by the modeling states as follows:

- Arizona—federated model
- Connecticut—hybrid model
- Colorado—federated model
- Nebraska—models that blended selected elements from banking, centralized, and/or federated models
- Oklahoma—federated model
- Washington—HRB model

The modeling states documented business models in a report that included the type of technical architecture, governance, current policy used or under development, and a summary of current baseline policies and procedures. The non-modeling states reviewed this report and then provided feedback and recommendations to the modeling states. The feedback and recommendations were directed at the current policy in use within the modeling state. These reports helped the team understand the diversity among the states, and that understanding drove the consensus-building discussions throughout the project. For further information, see Appendix A Description of the Collaborative States' Models.

2.5 Methodology

ASPC's methodology was organized into three major categories:[2] (1) environmental scan, used to identify best practice and policy, (2) use case documentation and analysis, and (3) negotiation and preparation of the Uniform Security Policy. Please see Appendix B for the flowchart that illustrates the methodology.

2.5.1 Environmental Scan

In conducting the environmental scan to establish best practice and policy, the collaborative reviewed nationally recognized literature and standards that impact authentication and audit. Consensus on terminology was achieved by compiling a common glossary of terms. Categories were developed to classify policies and practices and were used to develop a set of questions used to delineate current state practices and policies related to authentication and audit. The interim milestone for this process was the security policy template.

Literature Review

With the relevant standards identified, all members needed to achieve fluency in those standards. The documents that would be the basis for a common understanding of current security policies and standards were assigned to individual team members. Each member reviewed their specific documents and provided a summary document to inform the remaining team members. The summaries were posted to a shared workspace (ASPC Resource Library) where they could be reviewed and referenced.

The initial set of documents reviewed included:

1. A Framework of Principles and Resources for Addressing the 4As, excerpts from the Minnesota Privacy and Security Project Reports for the Privacy and Security Solutions for Interoperable Health Information Exchange Contract http://www.health.state.mn.us/e-health/mpsp/.
2. Markle Foundation, Connecting for Health Common Framework, *P7—Auditing Access To and Use of a Health Information Exchange.*

[2] See Appendix A for a flowchart of the ASPC process.

3. Markle Foundation, Connecting for Health Common Framework, *P5—Authentication of System Users.*
4. Department of Justice, Drug Enforcement Administration, 21 C.F.R. pts. 1300, 1304, 1306, and 1311 [Docket No. DEA–218P] RIN 1117–AA61, Electronic Prescriptions for Controlled Substances, AGENCY: Drug Enforcement Administration (DEA), Department of Justice. ACTION: Notice of Proposed Rulemaking.
5. HIMSS/GSA National e-Authentication Project Whitepaper, June, 2007. Copyright 2007 by the Healthcare Information and Management Systems Society.
6. HITSP Security and Privacy Technical Committee (SPI TC) Identity Credential Management Working Group Co-Chair Final Report, Mike Davis and Richard Thoreson, March 24, 2008.
7. E-Hi, Signatures and Identification for Everyone (SAFE), Interoperable Digital Identity Management in the Electronic Exchange of Health Information, An Expert Panel Report, December 17, 2007.
8. National Institute of Standards and Technology (NIST), NIST Special Publication 800-63-1.

Identification of Related Vocabulary and Standards

One of the earliest discussions centered on the importance of having all members of the collaborative share the same vocabulary. Four of the participating states had compiled glossaries. A HISPC Glossary had evolved from the work done in Phases I and II. Glossaries had also been assembled by standards groups, such as Healthcare Information Technology Standards Panel (HITSP). The collaborative reviewed these glossaries, extracted terms that were relevant to the project, and combined them into a working project-specific glossary.

As a working project-specific glossary, terms[3] were added as the team encountered them. Terms from the Nationwide Health Information Network (NHIN), International Organization for Standardization (ISO), NIST, and the Markle Foundation's Connecting for Health initiative were included. The team also incorporated acronyms that were used in the deliverables. Where multiple definitions for the same term were encountered, consensus was reached on the definition that most appropriately fit and only that definition was retained in the Glossary. The ASPC Glossary can be found in Appendix C.

Many team members were familiar with industry standards related to the secure exchange of health information. Early team discussions centered on these standards and identified those that would be important to consider as part of the collaborative's policy development work. The following organizations and their respective work products were reviewed:

Connecting for Health—http://www.connectingforhealth.org/

American Health Information Community (AHIC)—
http://www.hhs.gov/healthit/ahic/

[3] Such as those identified during the literature review and meetings.

Harmonized Use Case for Electronic Health Records (Laboratory Result Reporting) March 19, 2006 http://www.hhs.gov/healthit/usecases/documents/EHRLabUseCase.pdf

Medication Management Detailed Use Case June 18, 2007 http://www.hhs.gov/healthit/documents/UseCaseMM.pdf

The following use case was used in the Proof of Concept exercise:

Immunizations and Response Management Detailed Use Case March 21, 2008 http://www.hhs.gov/healthit/usecases/documents/IRMDetailed.pdf

Health Information Technology Standards Panel (HITSP)— http://www.hitsp.org/

The HITSP *Requirements, Design and Standards Selection Template* was used as a basis for the ASPC requirements analysis documents.

HITSP *Technical Note TN900—Security and Privacy* was considered during the Use Case Mapping work.

Integrating the Healthcare Enterprise (IHE)— http://www.ihe.net/

The IHE Cross Enterprise Document Sharing (XDS) Affinity Domain was used to identify the technical standards necessary to implement systems where the Minimum Security Policy Requirements for Authentication and Audit could be supported.

International Organization for Standardization (ISO)— http://www.iso.org/iso/home.htm

ISO/TS 22600-1:2006 Health informatics—Privilege management and access control—Part 1: Overview and policy management provided guidance to the collaborative. The standard is intended to support the needs of health care information sharing across unaffiliated providers of health care, health care organizations, health insurance companies, and their patients, staff members, and trading partners. It is also intended to support inquiries from both individuals and application systems.

Diagram materials were drawn from *IS01 Version 2.1.1* for the Laboratory Use Case and from *IS07 Version 1.0* for the Medication Management Use Case.

ASTM International—http://www.astm.org/

ASTM E2147—01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems was used in the development of the Environmental Scan and Focus Group tools.

Apgar & Associates—http://www.apgarandassoc.com/

Apgar & Associates *Information Security Audits* whitepaper was used in developing the Environmental Scan tools.

Existing State Authentication and Audit Policies

State teams and a limited number of local stakeholder groups gathered information that applied to authentication and audit policies and procedures. The information was limited to instances where a treating health care provider requests patient health information from a

state or local health care entity. For the purpose of this assessment, an entity includes a state or local geographic or regional health information exchange, hospital, clinic, or physician group.

The purpose of gathering information was to catalogue a set of policy elements that would apply to a request for protected health information across organizations and the policy's specific attributes, as they applied to authentication and audit. This information was essential to define a baseline need for the individual elements into a common "must/should/may" prioritization methodology. This set of policy elements established the groundwork for the development of criteria for the security policy template and served as an initial point of data for comparison later in the process.

The collaborative collected a variety of documents, from various sources, to use as references, including: E 2147—01 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, ISO/TS 22600-1: Health informatics—Privilege Management and Access Control, Responsible Audit Practices & Security/HIPAA Compliance (PowerPoint, Chris Apgar), Information Security Audits (White Paper, Chris Apgar).

The information was used to assess the types of authentication and audit policies utilized by HIOs and other entities electronically exchanging protected health information in the modeling states. A work group was established to identify a group of key topic areas related to the standards work. Security and privacy subject matter experts, including Richard Rubin of OneHealthPort, were then consulted to help synthesize and categorize the topics, which led to a draft structure for the scan.

This structure included the following five key categories:

I. Activating and Assigning an Account

II. Managing an Account

III. Entity Authentication—Verification of the Identity of a Provider requesting health information

IV. Data Transmission

V. Audit

This resulting draft was reviewed at an in-person collaborative meeting, where additional enhancements were added. These additions were based on information from the team's subject matter experts, and were informed by recent work done by HITSP, and the material included in the literature review. The team determined that both a short and a long version of the document would be useful. The long or detailed sets of elements were to be used in a limited number of stakeholder organizations that were being used as prototypes or models for HIE. The detailed sets of elements were also used with a limited number of stakeholders representing both forming and operational HIEs. The short version was used to validate the

responses from the detailed set of elements that were most critical to establishing a baseline reflecting current practices. The topic areas for provider authentication and audit reviewed organizational policies and processes included the following:

1. Health care provider *Use Agreement* content
2. *Registration* of the provider to become a subscriber of the health information organization
3. Process for *Verifying the Identity* of the provider
4. Identity Provisioning of the provider
5. Health information organization activities for *Maintenance* of health care provider system use
6. Access Control
7. Audit

Completing the environmental scan was labor intensive because the topic areas and elements focused on aspects of privacy and security that the states and HIOs had not yet addressed. The process helped those organizations identify omissions and additional issues that might need attention. In analyzing the scans as a group, the existing privacy and security environment for HIE was catalogued. The information collected by this process is summarized in Appendix D.

Initial Development of the Security Policy Template

Once the environmental scan was complete, the collaborative developed a preliminary security policy template listing each major component of authentication and audit and its subcomponents. The Environment Scan was used as the basis for this template, which ensured that we captured the same components that were used in the scan. Related definitions and examples were added from the NIST e-Authentication Publication 800-63 as well as the Markle Foundation, Connecting for Health, Common Framework. The security policy template provided a framework for discussions with a limited number of stakeholders in developing consensus within each state on minimum requirements. During these discussions some groups captured specific proposed business requirements. The security policy template helped define the parameters for the Uniform Security Policy. The process involved defining the crosswalks between the use case negotiated minimum policy requirements and the Security Policy Template. The Security Policy Template can be found in Appendix E.

2.5.2 Use Case Documentation and Analysis

Selection of Use Cases

The following AHIC use cases were selected to match the type of data the modeling states were exchanging or planning to exchange:

1. Harmonized Use Case for Electronic Health Records (Laboratory Result Reporting) March 19, 2006 http://www.hhs.gov/healthit/usecases/documents/EHRLabUseCase.pdf,
2. Medication Management Detailed Use Case June 18, 2007 http://www.hhs.gov/healthit/documents/UseCaseMM.pdf

The analysis conducted for the provider authentication and audit issues as applied to each of the use case transactions was performed by two or more states or jurisdictions operating under differing statutes or HIOs.

Development of the Use Case Data Collection Templates

The collaborative authored use case data collection templates to define the specific authentication and audit requirements for each use case. The templates provided a standard data collection tool for the modeling states as they mapped the use case(s) to their architecture.

The Use Case Data Collection Templates contained five related sections. Each section provided background and instructions for the assessment of policy requirements.

Section 1 provided a brief introduction to the document.

Section 2 of the template provided a general overview of the use case and the authentication and audit requirements specific to the use case.

Section 3 provided the policy and information requirements. This included the authentication and audit requirements for the intra- and/or interstate exchange relevant to the use case.

Section 4 described the use case actors/events/actions and mapped each to identified business requirements.

Section 5 described the AHIC-defined actors within a use case and required the modeling states to define their local business actor's specific to their HIO.

***Section* 6** defined the crosswalk between the HITSP Interoperability Specifications and the standards' implementation in authentication and audit policies.

The use case templates can be found in Appendix F.

Use Case Mapping

Each modeling state picked one or both use cases to map to its architecture. Colorado, Connecticut, Oklahoma, and Washington chose the Medication Management Detailed Use Case. Arizona, Colorado, Connecticut, and Nebraska chose the Harmonized Use Case for Electronic Health Records (Laboratory Result Reporting).

Modeling States' Minimum Policy Requirements

Each modeling state gathered information to determine its minimum policy requirements for authentication and audit given the conditions set forth in a selected use case. The data collected from the environmental scan questionnaire for states' HIO policy requirements for authentication and audit supplemented the authentication and audit requirements specific to the use case scenario. In the environmental scan the applicable vocabulary and technical standards were identified and discussion supported the team member's understanding of these parameters. The use case mapping exercise required the modeling states to evaluate the actors; authentication, audit, policy, system and data requirements; system activities; and policy implications in the relation to their architecture and the specific AHIC use case. The combined results of these analyses were used to synthesize the minimum policy requirements for authentication and audit for each modeling state.

Individual Requirements Review (IRR) Templates

The six modeling state's teams and HIOs completed use case templates. These templates were aggregated and the results were combined into a single document for use in review and negotiation. The IRR spreadsheet included data from the six states and represented a total of nine use case mappings, five on the EHR Laboratory Results Use Case and four on the Medication Management Use Case. The IRR incorporated specific detail on 384 individual authentication and audit security requirements.

2.5.3 Negotiation and Policy Development

Negotiation

The detail[4] provided in the IRR had to be distilled into minimum policy requirements for authentication and audit. To effectively and efficiently synthesize these requirements, the collaborative sought help from a state not active in the negotiations. The Commonwealth of Virginia's state team served as the negotiation facilitator and authored documentation of the process. The negotiating team was made up of representatives from each modeling state, and the team progressed sequentially through the IRR tables for the five template categories—Authentication, Audit, Data, System, and Policy. At the successful end of the negotiation meetings, all states agreed to 205 of the minimum policy requirements proposed, and a final IRR table was produced and circulated back to the team. Only minimum policy requirements that all modeling states agreed to were added to the final authentication and audit security policy. If no consensus was reached, the policy was not included. At the end of the negotiation process, the completed IRR identified all of the

[4] The complexity of collecting the individual requirements might have been reduced with the use of a typology of architecture cross tabulated with each requirement. For example, inclusion of a patient health record (PHR) would have different security requirements than a system that provided access only to health care providers.

ASPC's Minimum Policy Requirements and became the basis for the drafting of the Uniform Security Policy. The IRR can be found in Appendix G.

Development of the Uniform Security Policy

The Security Policy Template was integrated with the final negotiated IRR document to produce the Uniform Security Policy. Requirements were grouped and provided the outline for the Uniform Security Policy. The Uniform Security Policy can be found in Appendix H.

Development of the Guide to Adoption of Uniform Security Policy

An original deliverable, the Guide to Adoption of Uniform Security Policy was designed to summarize the process that HIOs would need to address to adopt the minimum policy requirements through a consensus process. The Guide had two primary objectives:

To provide a framework for establishing interstate authentication and audit policies using minimum policies vetted by a multistate collaborative effort.

To demonstrate how alignment of local policies with broadly accepted policies can facilitate health information exchange agreements.

The Guide to Adoption of Uniform Security Policy contains information about the process for adoption. It addresses the challenges in driving adoption of the Uniform Security Policy and presents strategies for success. The Guide provides a framework to prepare organizations to adopt or change the policy. A process checklist and glossary are included. A resource list is offered for prospective users of the guide.

The Adoption of Uniform Security Policy Guide is intended to be used as a manual to adopt the policy. It provides an adaptation of the collaborative's work to be used to facilitate HIE with best practice policies for authentication and audit.

2.5.4 Legal Working Group Process

The legal advisor to the ASPC, Kristen Rosati, a partner at Coppersmith Gordon Schermer & Brockelman PLC ("Coppersmith Gordon"), provided feedback on all documentation and the legal issues involved. The full legal review can be found in Appendix I. In the interim and final legal reports, Ms. Rosati discussed federal and potential state legal issues that affect key components of authentication and audit policies in HIE. These include the following issues:

Federal laws:

- HIPAA Privacy and Security (including new developments in the HITECH Act)
- Clinical Laboratory Improvement Amendments (CLIA)
- Substance abuse treatment regulations
- FTC Red Flag Rules

- E-SIGN
- Proposed DEA regulations

State laws:

- Laws that impose authentication and audit requirements in health care
- Laws that impose authentication and audit requirements for all businesses
- Medical record confidentiality statutes
- Laws regarding social security numbers
- Tort laws, including tortuous invasion of privacy, state constitutional right to privacy, negligence claims with HIPAA as the standard of care, and negligence per se claims

2.6 Stakeholder Review

The Uniform Security Policy and the Guide to Adoption of Uniform Security Policy were reviewed by stakeholder groups within modeling states. Comments focused on the utility and applicability of each and were used to revise portions of the Uniform Security Policy and the Guide to Adoption of Uniform Security Policy. The general tenor of these comments was supportive and encouraging.

Specifically, ASPC sent a draft of the Uniform Security Policy to Stakeholders in 11 states on February 6, 2009. The policy was distributed through 11 different states and stakeholders were requested to vet the policy against existing or planned security policies, to see how best they could work with an exchange with another HIO, both intra and interstate. Stakeholder comments and recommendations can be found in Appendix J.

2.7 Findings

The ASPC has successfully distilled common requirements for secure HIE that remain negotiable. The basic policy offered in these documents will serve as a foundation to establish trusted cross-state model neutral policy for exchange.

The Uniform Security Policy will help establish common business practices for registering and authenticating users and providing specified audit parameters, to benefit both the individual users and the participating organizations.

Adoption of technology standards and associated policies for trusted cross-HIO exchange requires tools to understand requirements, test functionality and a guide to successfully transition from current models.

2.8 Lessons Learned

To responsibly articulate a model security policy for trusted multistate health information exchange is a significant undertaking. The variability in architectures, methods of exchange,

organizations, processes and other elements served to complicate the environmental scan. The elements of a security policy, authorization, authentication, access, and audit are not truly discrete in practice and have many interdependencies.

To facilitate the success of future efforts, the scope of the project needs to be very clearly defined initially and methodology specified with concrete delineation of the work to be completed. Scope creep occurs without intention. For example, when the collaborative addressed system and data authentication, there were new requirements in the audit parameters. The minimum necessary to assure audit component compliance meant that timestamp needed to be communicated and stored to run a valid audit report. Another example was that consumer matching is critical to authentication and audit and was outside of the project scope.

Consensus-based decision making was limited by attempts to negotiate model neutral policy requirements. This was evident with the health record bank patient/consumer controlled model. Specifically, the Washington Health Record Bank (HRB) model for interoperability gives patients web-based electronic access to their medical data from multiple sources and the patient controls access. The patient also supplies information to validate medications and advance directives. The patient-controlled HRB fosters patient activation and is designed to be shared electronically by the patient action. To design universal authentication and audit requirements that would fit this model and a provider-to-provider exchange lead to fewer agreed-to elements in the Uniform Security Policy. Developing a typology of architectures and functionalities to overlay onto the security requirements would expedite future analysis.

Policies cannot be static if they are to address the changing landscape of health information exchange. Formulation of policies that conform to current standards also must address the need to evolve with changes across the industry. For audit, there were too many variations in the methods for identifying entities responsible. The specificity needed to identify what has been transmitted (data), to which entities (system), and what record (audit) is to be held in which location are all subject to industry practice and standards that are still evolving. The responsibility for tracking audit information is architecture dependent and rules about data transmission are subject to interpretation.

The following elements were critical to the collaborative's success and were essential to developing the policy requirements:

- a common glossary of terms and definitions,
- a baseline of existing policies within each collaborative state, that accurately represented the practices and procedures of the negotiating parties, and
- identification of relevant standards and detailed documentation of their relationship to the HIO policies being developed.

Concepts that were helpful in reaching consensus were:

- An understanding that current common practices and the current level of technological development may fall short of the ideal for effective, reasonably priced and secure exchange of health information. Policies must be established to support the present reality and must be improved cyclically as HIE processes evolve.
- Acknowledgement of the necessity for a minimum policy that is acceptable to organizations whose size, available resources, and complexity vary widely. Organizations will vary in their determination of what policies they will adopt, and what minimum policies they require their exchange partners to have in place. The Uniform Security Policy is offered as a best practice solution.
- Outreach should occur throughout the process to stakeholders responsible for policy implementation.

3. NEXT STEPS

Since health information technology is presumed to be a significant component in plans to improve the health care system, the importance of privacy and security has been preeminent. However, the methods for consistent application of best security practices across organizations have not been addressed. The Adoption of Standard Policies Collaborative (ASPC) has provided the foundation for authentication and audit for treatment purposes. The Guide to Adoption of Uniform Security Policy provides a framework build consensus on privacy and security practices to support the electronic exchange of health information.

Policies for interstate exchange of health information for authentication and audit are a beginning. The other two security domains, authorization and access, are yet to be addressed. The framework used by the Adoption of Standard Policies Collaborative provides a solid basis for developing standard policies for authorization and access.

Next steps in developing standard security policies and practices include evaluating and testing the viability of this framework as it is adopted and implemented for interstate health information exchange. No matter what legal mechanisms are used to establish a network of trust among health information exchanges, specificity is required for security policies and practices. The framework offered here is intended as a starting point to be augmented, expanded, and tested as health information exchange becomes the modality to provide accurate clinical information at the point of care to improve health care quality.

ASPC recommends the following:

- Test the framework in environments that implement and assess the viability of the standard policies for authentication and audit.
- Document the types of use cases and transactions that occur in health information exchanges, to provide paradigms for policy and practice development for authorization, access, disaster recovery, archiving, and other intersecting domains.
- Work with AHIC's successor to share information and products developed in the health information exchanges, providing expert assistance to expedite health information technology adoption, and to leverage lessons learned for future application.
- Establish or designate a rigorous and transparent policy review process, using the standards development organizations' methodologies and practices.
- Standardize testing of the technology supporting these policies for the vendor market.
- Evaluate the capacity to adhere to and support uniform security policies in the certification of health information exchanges.

- Provide funding for prototypes to test policy standards as they are technologically implemented.

4. CONCLUSION

The widespread adoption of common standards-based security policies is essential to developing the trust relationships upon which all health information exchange efforts depend. The legal and policy context of health information exchange is found in federal rules and law and is further modified by state laws. The technical foundations for secure and private transport of health information are principles used to control:

- Authorization—who gets to view and edit the data.
- Authentication—how we know them to be who they assert to be.
- Access—what data they can acquire.
- Audit—the record of who has seen and changed what data.

These foundations are often referred to as the 4A's. The application of these principles is specified in legal agreements among organizations, health information exchanges, and the Nationwide Health Information Network. This network of trust will benefit from specified standard policies like those recommended by the Adoption of Standard Policies Collaborative.

APPENDICES

APPENDIX A:
DESCRIPTION OF THE COLLABORATIVE STATES' MODELS

The following state-by-state summaries provide additional details about the HIO s used, illustrate the breadth of HIO environments included in the ASPC work, and identify the significant resources and expertise provided by both Modeling and non-Modeling states.

Arizona: The state's focus is driven by health care costs and specifically by Medicaid expenses administered by the state government. The Arizona Health Care Cost Containment System (AHCCCS), the state's single Medicaid agency, used a Medicaid Transformation Grant to develop and implement an open source web-based health information exchange utility to give all Medicaid providers instant access to patient health information at the point of service. The funds are being used to support the planning, design, development, testing, implementation, and evaluation of the AHCCCS Arizona Medical Information Exchange (AMIE) that was used as the Arizona HIO.

Colorado: Colorado uses a federated HIO and has four partners working to exchange health information through a central site that offers secure hosted services. The HIE has been incorporated as a nonprofit organization, with the Governor and his cabinet closely involved with the HIE. Currently, there are multiple efforts to expand the partnership beyond the original four partners funded by Agency for Healthcare Research and Quality (AHRQ) to build an HIE demonstration. The original partners were (1) Denver Health, (2) Kaiser Permanente, (3) the Children's Hospital and (4) the University of Colorado Hospital. Additional groups now involved include the Colorado Community Health Network composed of 14 federally qualified health centers; several rural critical access hospitals; the Colorado Clinical Guidelines Collaborative; and the Healthcare Policy and Financing Agency, which is the administrator for Medicaid and the Colorado State Child Health Insurance Program.

Connecticut: As a hybrid HIO state, Connecticut exchanges protected health information utilizing elements from the state, regional and private sector. This includes the Department of Public Health (Primary Care Physician Registry, Immunizations), Department of Social Services (Title 19 Practitioner Registry, Medications), state RHIOs (Patient Index, Record Locator), community RHIOs (Patient Index, Provider Registry, Clinical Data), and private health care providers (Patient Index, Provider Registry, Continuity of Care, Laboratory). Participants submit clinical data to a centralized regional repository responsible for data management of patient identification, storage, system management, security and privacy. The regional repositories are connected via a centralized Master Patient Index (MPI) or Record Locator Service (RLS).

Maryland: As one of the non-Modeling states in the ASPC, Maryland has embarked on building a statewide HIE that is a patient-centric, clinical data information-sharing utility where privacy and security are vital virtues. In Maryland's HIO, the information belongs to

the patient. Consumers may access their information, have substantial control over the flow of that information, and have a key voice in developing information exchange policies. The architecture is a combination of a federated HIE HIO with health record banks tethered to the utility.

Nebraska: Nebraska is the one state in the ASPC that currently has multiple HIOs in various stages of development and implementation. They include federated, banking, centralized, and hybrid HIO s. One HIO has been exchanging data for a number of months and another is in the pilot phase of exchanging electronic health information. The state government has adopted a facilitative and advisory approach to statewide HIOs. The Governor's office has established an e-Health Council that has both public and private representation and is advised by the state's HISPC workgroups.

Ohio: Ohio is a non-Modeling state for the ASPC, and has reviewed all of the documentation of the collaborative. Ohio has extensive experience with health information exchange as it is home to three operating health information exchanges: HealthBridge in the greater Cincinnati area, HealthLink RHIO in the Dayton area, and Collaborating Communities Health Information Exchange (CCHIE) in the Springfield area. In Cleveland, the North East Ohio RHIO (NEORHIO) has organized a governing structure. HealthBridge, HealthLink and the Cleveland Clinic are all participants in the Nationwide Health Information Network (NHIN). All of the Ohio HIOs use different business HIO s and technologies. HealthBridge pushes data to health care providers using the vendor, Axolotl, and provides clinical messaging with no central repository of data. CCHIE uses the same technology and HIO. HealthBridge's other services include an EMR lite and interfaces to integrate lab data into many vended EHR systems. HealthBridge's data is organized by provider. HealthLink uses a patient and household-centric record hosted on a Microsoft platform. Wright State, the administrative home for the HealthLink RHIO, has a patent pending on the HIEx™ system that includes eligibility, social services and a clinical record that includes problems, medications, procedures and immunizations. The Cleveland Clinic is on the Epic system and uses Northrop Grumman for the NHIN interface for their integrated delivery system. The experience across the state has included much discussion and practice in health information privacy and security and that has informed the Ohio team's participation in the collaborative.

Oklahoma: Oklahoma uses a federated HIO for the state agency RHIO that receives claims and eligibility data from the state healthcare authority and other state agencies, as well as personal health history from consumers' personal health records. The state RHIO sends claims and eligibility data to both provider electronic health records (EHRs) and rural provider web-based EHRs. The state HIE uses a state agency Master Patient Index, a Record Locater Service, and a consolidated provider master.

Utah: Utah, as a non-Modeling state, supported the ASPC by playing a major role in the development of the templates and tools for data collection and analysis. Its work in developing the Use Case Template and aggregating data were essential to the project's success. Utah is in the process of expanding statewide capacity for clinical exchange, and has a vested interest in staying involved with the development work being completed by the HISPC Phase III Collaboratives.

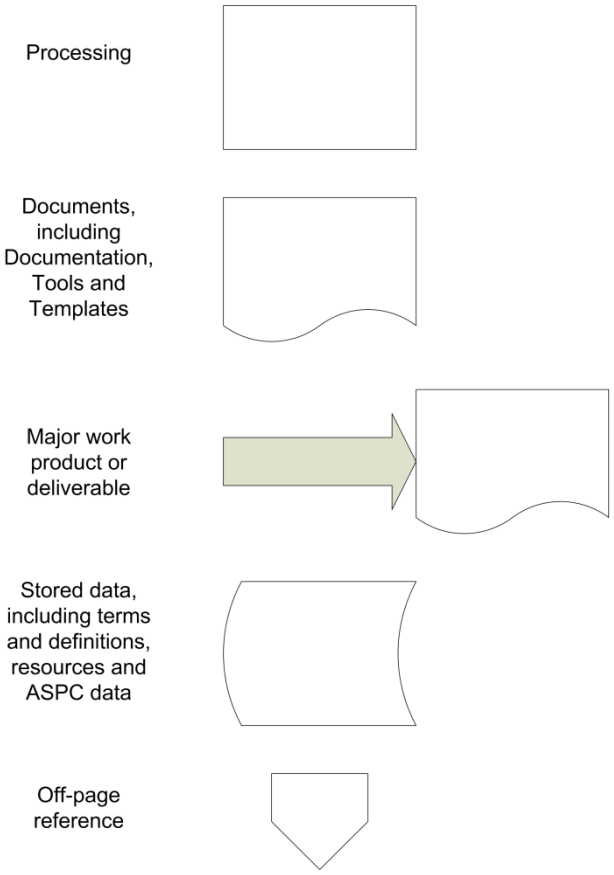
Virginia: Virginia, a non-Modeling state, contributed to the ASPC by leveraging the expertise it has to draw from two functional RHIOs, one operating a hybrid HIO environment and one operating using a federated HIO. In the hybrid HIO, participants can choose to store their records in the RHIO's Document Repository or keep their records to themselves by being their own firewalls. The documents are registered with the RHIO and are available for queries.

Washington: Washington employs a banking HIO based on the recommendation of their legislature that their Health Information Infrastructure Advisory Board (HIIAB) adopt a consumer-controlled, online, personalized health record bank (HRB) as the HIO for assuring that key data elements from a patient's health record are available to providers at the point-of-care. The HIIAB was made up of 12 volunteer business, academic, and policy leaders in the state that represented a wide array of stakeholders. Its mission was to develop a strategy for the adoption and use of electronic medical records and health information technology. The HRB was defined by the HIIAB as an independent organization providing a secure electronic repository for storing and maintaining an individual's lifetime health and medical records. The HIIAB also designated a limited number of high-priority data elements including (1) medication lists, (2) allergies, (3) advance directives, and (4) immunizations to be pilot-tested first, with the understanding that additional data elements would be added once a proof-of-concept phase was complete. The HRB is designed to store copies of records from multiple sources and ensure that the individual always has complete control over who accesses their information.

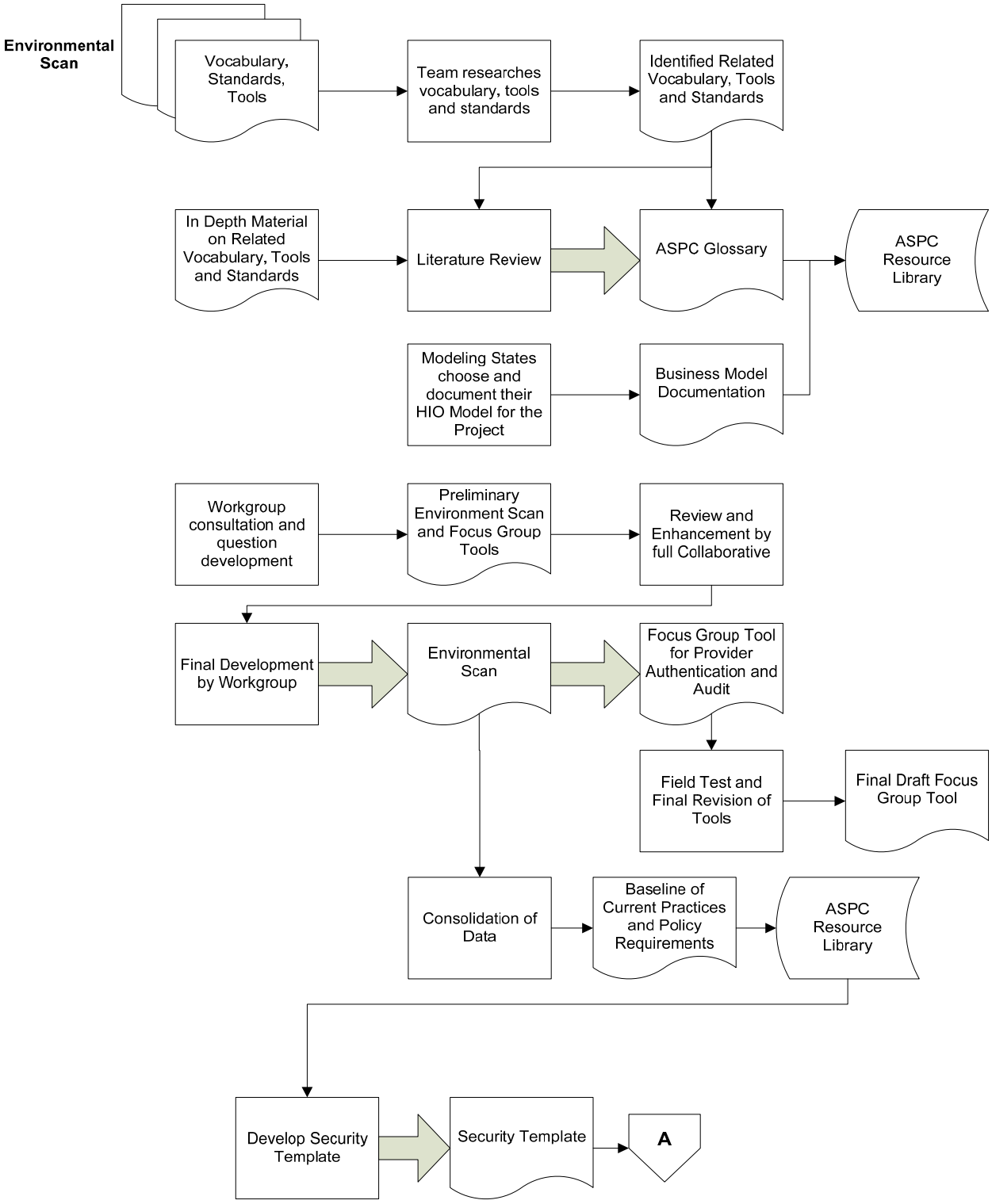
APPENDIX B:
FLOWCHART OF COLLABORATIVE PROCESS

The following flowchart provides a visual outline of the collaborative process the ASPC followed. It demonstrates critical relationships between elements of the process and communicates the important role that established standards, reputable work by other organizations and legal review played in the creation of the Uniform Security Policy.

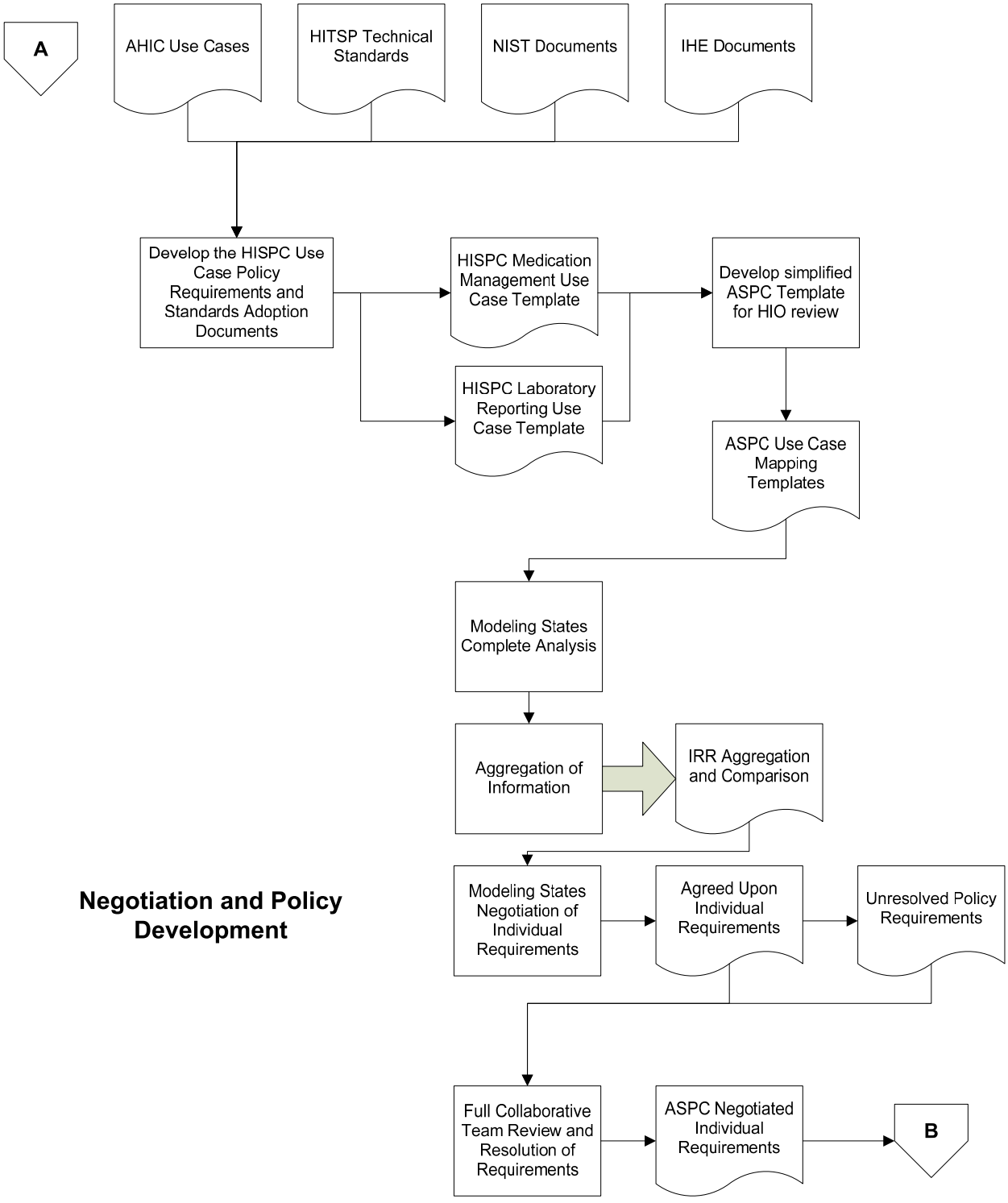
Key symbols used to outline the process include the following:



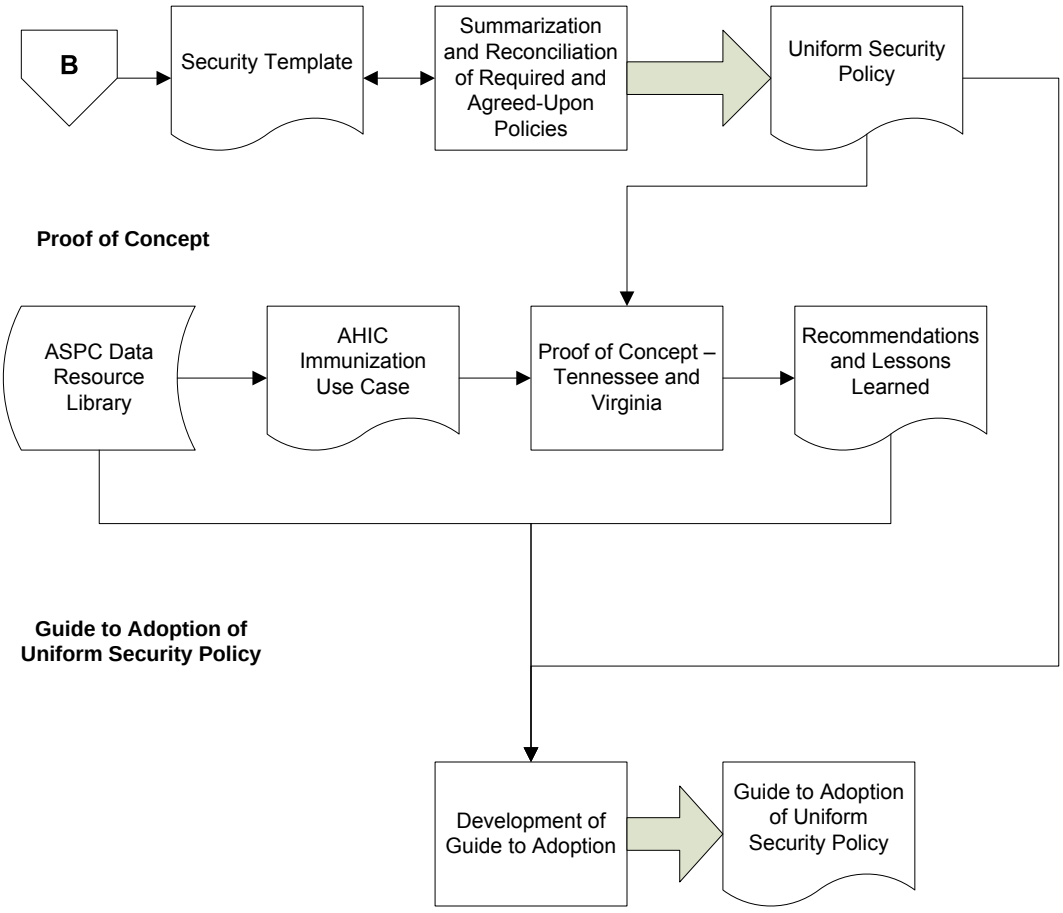
Methodology



Use Case Documentation and Analysis



Negotiation and Policy Development (cont.)



APPENDIX C:
ASPC GLOSSARY AND ABBREVIATIONS

Table C-1. ASPC Glossary and Abbreviations

Term	Definition	Source of Definition
4 A's	Authorization, Authentication, Access, and Audit	HIPAA
911 Telecommunicator	As used by 911 services, a person who is trained and employed in public safety telecommunications. The term applies to call takers, dispatchers, radio operators, data terminal operators, or any combination of such functions in a Public Safety Answering Point (PSAP).	Emergency Responder Use Case
Access Control	Prevention of unauthorized use of information assets (ISO 7498-2). It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises (OASIS XACML).	HITSP Glossary
Accountability	Property ensures that the actions of an entity may be traced to that entity.	[ISO 7498-2:1989]
Affinity Domain	A group of health care enterprises that have agreed to work together using a common set of policies and infrastructure	IHE IT Infrastructure Technical Framework-1:10
AHIC	American Health Information Community.	Emergency Responder Use Case
Allergy	Hypersensitivity caused by exposure to a particular antigen (allergen) resulting in a marked increase in reactivity to that antigen on subsequent exposure, sometimes resulting in harmful immunologic consequences.	Medication Management Use Case
Ambulatory Care	Any medical care delivered on an outpatient basis. Sites where ambulatory care can be delivered include physician offices, hospital emergency departments, and urgent care centers.	Medication Management Use Case
Applicant	A party undergoing the processes of registration and identity proofing.	NIST 800-63-1 *Draft Electronic Authentication Guideline* 2/20/08
Assertion	A statement from a Verifier to a Relying Party that contains identity information about a Subscriber. Assertions may also contain verified attributes.	NIST 800-63-1

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Assurance	In the context of NIST SP 800-63, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.	NIST 800-63-1
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.	NIST 800-63-1
Audit Trail and Node Authentication (ATNA)	Establishes the characteristics of a Basic Secure Node: 1. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. 2. It defines basic auditing requirements for the node. 3. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. 4. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially actor-specific requirements. The Radiology Audit Trail option in the IHE Radiology Technical Framework is an example of such an extension.	[Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)]
Authentication	The process of establishing confidence in the identity of users or information systems.	NIST 800-63-1
Authentication Protocol	A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.	NIST 800-63-1
Authorization	The granting of rights, which includes the granting of access based on access rights.	[ISO 7498-2:1989]

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Availability	The property of being accessible and useable upon demand by an authorized entity.	[ISO 7498-2:1989]
Baseline	A usually initial set of critical observations or data used for comparison or a control; a starting point.	Merriam-Webster Online Dictionary
Battalion Aid Station	A field medical unit. The first organized aid station a soldier/marine will see when transported from the care of the front-line corpsmen.	Emergency Responder Use Case
Biometrics	Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.	NIST 800-63-1
Care	Relieving the suffering of individuals, families, communities, and populations by providing, protecting, promoting, and advocating the optimization of health and abilities.	Emergency Responder, Medication Management Use Case
CCHIT	Certification Commission for Healthcare Information Technology.	Medication Management
Certificate Revocation List	A list of revoked public key certificates created and digitally signed by a Certification Authority.	NIST 800-63-1
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.	NIST 800-63-1
Challenge-response protocol	An authentication protocol where the Verifier sends the Claimant a challenge (usually a random value or a nonce) that the Claimant combines with a secret (such as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the Verifier. The Verifier can independently verify the response generated by the Claimant (such as by recomputing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret.	NIST 800-63-1
Claimant	A party whose identity is to be verified using an authentication protocol.	NIST 800-63-1
Clinicians	Health care providers with patient care responsibilities, including physicians, advanced practice nurses, physician assistants, nurses, and other credentialed personnel involved in treating patients.	Medication Management Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
CMS	Centers for Medicare & Medicaid Services, a federal agency within the Department of Health and Human Services.	Medication Management Use Case
Command and Control Center	The location where the exercise of authority and direction by a properly designated Incident Commander over assigned and attached forces occurs in the accomplishment of the mission.	Emergency Responder Use Case
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	[ISO 7498-2:1989] 45 CFR § 164.304 Definitions
Consistent Time	Mechanisms to synchronize the time base between multiple actors and computers. Various infrastructure, security, and acquisition profiles require use of a consistent time base on multiple computers. The Consistent Time Profile provides a median synchronization error of less than 1 second.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)
Consumers	Members of the public who may receive health care services. These individuals may include: caregivers, patient advocates, surrogates, family members, and other parties who may be acting for, or in support of, a patient in the activities of receiving health care.	Medication Management Use Case
Contraindication Alerts	Notifications that can be provided to a provider or pharmacist providing warnings concerning drug interactions with other drugs, indicated allergies, and other situations.	Medication Management Use Case
Coroner	A public official whose primary function is to investigate by inquest any death not deemed to be of natural causes. This is sometimes an elected position, and the individual may not have a medical background, as required for a Medical Examiner.	Emergency Responder Use Case
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.	NIST 800-63-1
Credentialed Personnel	A degree, certificate, or award that recognizes a course of study taken in a certain area, and acknowledges the skills, knowledge, and competencies acquired. In the health field, personnel are usually required to register with the credentialing body or institution not only in their discipline, but also in the state, locality, and institution where they practice.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Credential Service Provider (CSP)	A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.	NIST 800-63-1
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall coincide with the minimum requirements stated in table 2 of NIST SP [800-57] part 1. See also Asymmetric keys, Symmetric key.	NIST 800-63-1
Cryptographic Token	A token where the secret is a cryptographic key.	NIST 800-63-1
CT-HISPI	Connecticut Health Information Security and Privacy Initiative.	N/A
Current Hospital Medication List	The patient medication list initiated at admission and modified as additional medications are ordered during a hospital stay.	Medication Management Use Case
Current Medication List	A list of medications for which a consumer has an active prescription; this information is frequently consulted by a clinician while providing care and is especially important during transitions in care from one site, setting, or level of care to another. Clinicians are assisted in care management decisions if the current medication list includes patient-reported use of non-prescription medications such as over-the-counter drugs and remedies such as herbal and homeopathic supplements.	Medication Management Use Case
Data Integrity	Property that data has not been altered or destroyed in an unauthorized manner.	[ISO 7498-2:1989]
Data Origin Authentication	Corroboration that the source of data received is as claimed.	[ISO 7498-2:1989]
Definitive Care	Definitive care is provided by clinical care non-emergency department (ED) personnel providing acute, rehabilitative, or custodial care. They evaluate and treat patients in locations other than an ED, such as specialty hospitals, dialysis centers, nursing homes, hospices, and other facilities. They may include physicians, nurses, respiratory therapists, technicians, and many others.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Definitive Care Facility (e.g., Facility in the Definitive Care System)	A facility in the comprehensive health care system that provides health care to patients excluding that provided in the ED. Typically, facilities in the comprehensive care system offer more specialized care than that offered in the ED. Patients may access facilities in the comprehensive care system directly, be discharged to them after leaving the ED, or be discharged from one facility in the comprehensive care system to another.	Emergency Responder Use Case
Demographic Information	Basic patient identifying information such as name, age, gender, and primary language spoken.	Emergency Responder Use Case
Department of Health and Human Services (HHS)	This is the federal agency responsible for human health, and has oversight over many other federal agencies such as FDA, the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), CMS, the Agency for Health Research and Quality (AHRQ), the Substance Abuse and Mental Health Services Administration (SAMHSA), and others.	Medication Management Use Case
Designated Receiving Facility	A designated receiving facility is a facility where a patient will be sent for the next stage of treatment.	Emergency Responder Use Case
DHS	The U.S. Department of Homeland Security.	Emergency Responder Use Case
Diagnostic Test Results	Results of any diagnostic tests ordered: blood or urine tests, X-rays, EKG, etc.	Emergency Responder Use Case
Dietary Supplement	A product taken by mouth that contains a “dietary ingredient” intended to supplement the diet. These ingredients may include vitamins, minerals, herbs or other botanicals, or other substances.	Medication Management Use Case
Digital Identity	A digital representation of a set of claims by one party about itself or another digital subject.	ASPC Negotiated definition
Digital Signature	Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.	[ISO 7498-2:1989]
Disaster Medical Assistance Teams	Teams of medical professionals organized by the National Disaster Medical System pre-designated to respond to disasters with specific capabilities.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Discharge Plan	A synopsis of the treatments recommended for the patient to complete upon leaving the institution, including medications, medical appointments, other therapeutic interventions, further diagnostic studies, and recommendations for follow-up.	Emergency Responder Use Case
Discharge Prescription	A prescription written at the end of a hospital stay as a patient is released to self-care or the care of another, including a provider such as a primary care provider or a long-term care facility provider.	Medication Management Use Case
DMORT	Disaster Mortuary Operational Response Teams.	Emergency Responder Use Case
DoD	The Department of Defense.	Emergency Responder Use Case
DOT	The Department of Transportation.	Emergency Responder Use Case
Drug Knowledge Suppliers	Organizations that maintain and provide reference information on drugs that is used to provide clinical content in pharmacy systems and EHRs. Drug reference information provides the clinical content for medication screening for possible contraindications such as drug-drug, drug-allergy, or drug-diagnosis interactions and inappropriate dosing. It also can provide assistance in selecting appropriate medications and quick access to monographs and other reference information. Drug Knowledge Suppliers can also provide new warnings, prescribing limitations, similar communications, and patient education information.	Medication Management Use Case
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.	NIST 800-63-1
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a Subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.	NIST 800-63-1
Electronic Health Record	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.	National Alliance For Health Information Technology

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Electronic Health Record (EHR) System Suppliers	Organizations that provide specific EHR solutions to clinicians and patients such as software applications and software services. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities.	Immunization Use Case
Electronic Medical Record	An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.	National Alliance For Health Information Technology
Emergency Care	Emergency care is provided by clinical care personnel operating in a Medical Treatment Facility (MTF). They usually work in an ED or equivalent military facility, evaluating and or treating patients before they are discharged, admitted to an inpatient facility, or deceased. They may include physicians, advanced practice nurses (e.g., nurse practitioners, nurse anesthetists), emergency nurses, physician's assistants, and military corpsmen.	Emergency Responder Use Case
Emergency Care Record	Record of patient care given in an ED. May be in an electronic format.	Emergency Responder Use Case
Emergency Contact Information/Next of Kin Registries	An emergency contact information/next-of-kin registry is an organized system for the registration, storage, retrieval, and dissemination of emergency contact information for individual persons.	Emergency Responder Use Case
Emergency Dispatch Center	The location where emergency resources at the local level are managed and dispatched; also known as a 911 Call Center or Public Safety Answering Point (PSAP).	Emergency Responder Use Case
Emergency Medical Dispatcher	A specially trained public safety telecommunicator with the specific emergency knowledge essential for the appropriate and efficient functioning of emergency medical dispatching.	Emergency Responder Use Case
Emergency Medical Systems (EMS)	The organized arrangement of field and hospital clinicians, response and transport vehicles, protocols and procedures responsible for patient care and transport from time of injury/illness through the delivery of emergency care.	Emergency Responder Use Case
Emergency Medical Technician (EMT)	There are four license levels defined by DOT. They are Medical First Responder (MFR), Emergency Medical Technician-Basic (EMT, EMT-B, Basic), EMT-Intermediate (EMT-I, Intermediate, EMT-S, Specialist), and EMT-Paramedic (EMT-P, Paramedic, Advanced EMT, AEMT).	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Emergency Operations Center (EOC)	An EOC is the physical location where various organizations come together under the direction of EOM during an emergency to coordinate response and recovery actions and resources. These centers may alternatively be called command centers, situation rooms, war rooms, crisis management centers, or other similar terms.	Emergency Responder Use Case
Emergency Operations Center systems	IT systems supporting the EOC. They manage the situational awareness, resource management and other functions.	Emergency Responder Use Case
Emergency Operations Management (EOM)	Emergency operations management personnel are involved in planning, staffing, and information collection activities at the institution, community, or regional level to implement measures that will save the most patients. They track the status of available resources; allocate patients to the facilities best suited to care for them; and arrange staffing, logistics, and supplies to care for patients. They may include disaster responders; patient tracking personnel who help provide family members with information on the status and location of patients; hospital planners; nursing supervisors; EMS managers/patient regulators who determine where ambulances take patients; other National Incident Management System (NIMS) roles; and emergency managers and planners.	Emergency Responder Use Case
Episode of Care	A patient health problem starting from the first encounter to discharge, release to the care of another facility, or departure against medical advice.	Emergency Responder Use Case
ePrescribing	The process of using electronic means to transfer information between provider and pharmacist regarding a prescription.	Medication Management Use Case
Evacuation Center	Shelter that provides a temporary “safe haven” to evacuated or displaced populations. Evacuation centers are austere and not intended for long-term occupancy. They are usually established by local governmental entities or organizations such as the American Red Cross.	Emergency Responder Use Case
Fatality Management Systems	IT systems used in support of the Medical Examiner/fatality manager in support of their mandated duties.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
FDA	Food and Drug Administration; a federal agency within the Department of Health and Human Services responsible for the safety regulation of foods, dietary supplements, vaccines, drugs, medical devices, veterinary products, biological medical products, blood products, and cosmetics.	Immunization, Medication Management Use Case
Federal Medical Station	A unit intended to provide a federal deployable medical capability (equipment, material, pharmaceuticals) to assist hospitals in meeting needed surge requirements, though in an emergency they may assist state and local governments.	Emergency Responder Use Case
FEMA	The Federal Emergency Management Agency.	Emergency Responder Use Case
FHA	Federal Health Architecture.	Emergency Responder Use Case
First Responder	Police and fire, whose primary expertise is something other than medical, but who can provide basic first aid.	Emergency Responder Use Case
Formulary	A list of medication that can be prescribed and is allowable under a set of restrictions such as available in the pharmacy or covered by a health plan.	Medication Management Use Case
Functional Roles	Functional roles reflect the essential business functions that need to be performed. Functional roles are defined by a set of standard health care tasks (e.g., neurologist).	Neuman/Strembeck
Government Agencies	Federal, local, state, territorial, or tribal departments within the United States government responsible for the oversight and administration of a specific function; government agencies may include: Department of Health and Human Services (DHHS), Food & Drug Administration (FDA), Centers for Disease Control and Prevention (CDC), Centers for Medicare & Medicaid Services (CMS), Department of Defense (DoD), Department of Veterans Affairs (VA), Indian Health Services (IHS), and Department of Homeland Security (DHS).	Immunization Use Case
Health Information Exchange	The electronic movement of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology
Health Information Organization	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.	National Alliance For Health Information Technology

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Health Information Service Providers	A network service provider that enables or oversees the access to and exchange of health information, in a secure manner, for the purpose of supporting clinician and consumer needs.	Emergency Responder Use Case
Health Information Services (HIS)	Services provided by Health Information Networks for information exchange and interoperability in a local market.	Emergency Responder Use Case
Health Record Banks	Entities/mechanisms for holding an individual's lifetime health records. This information may be personally controlled and may reside in various settings such as hospitals, doctor's offices, clinics, etc.	Immunization Use Case
Health Registries	A health registry is an organized system for the collection, storage, retrieval, analysis, and dissemination of information on individual persons who have either a particular disease, a condition (e.g., a risk factor) that predisposes to the occurrence of a health-related event, or prior exposure to substances (or circumstances) known or suspected to cause adverse health effects.	Emergency Responder Use Case
Health Researchers	Organizations or individuals who normally perform analysis of health trend information. They normally use anonymized patient information in their studies.	Emergency Responder Use Case
Healthcare Entities	Organizations that are engaged in or support the delivery of health care. These organizations could include hospitals, ambulatory clinics, long-term care facilities, community-based health care organizations, employers/occupational health programs, school health programs, dental clinics, psychology clinics, care delivery organizations, pharmacies, home health agencies, hospice care providers, airport clinics, mass vaccination sites, public health agencies, retail store clinics, and other health care facilities.	Immunization, Medication Management Use Case
Healthcare Organization	Officially registered organization that has a main activity related to health care services or health promotion. EXAMPLES: Hospitals, Internet health care website providers and health care research institutions. NOTE 1: The organization is recognized to be legally liable for its activities, but need not be registered for its specific role in health. NOTE 2: An internal part of an organization is called an organizational unit, as in X.501.	[ISO IS 17090]

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Health Care Payors	Insurers, including health plans, self-insured employer plans, and third party administrators, providing health care benefits to enrolled members and reimbursing provider organizations. As part of this role, they provide information on eligibility and coverage for individual consumers, as well as claims-based information on consumer medication history. Case management or disease management may also be supported.	Immunization, Medication Management Use Case
HIMSS	The Healthcare Information and Management Systems Society is the health care industry's membership organization exclusively focused on providing global leadership for the optimal use of health care information technology and management systems for the betterment of health care.	The Healthcare Information and Management System Society
HISPC	Health Information Security and Privacy Collaborative.	N/A
HITSP	The American National Standards Institute (ANSI) Healthcare Information Technology Standards Panel; a body created in 2005 in an effort to promote interoperability and harmonization of health care information technology through standards that would serve as a cooperative partnership between the public and private sectors.	Immunization, Medication Management Use Case
Identification	Performance of tests to enable a data processing system to recognize entities.	[ISO/IEC 2382-8:1998]
Identifier	Piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator.	[ENV 13608-1]
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.	NIST 800-63-1
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.	NIST 800-63-1

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
IHE	Integrating the Healthcare Enterprise (IHE) is an initiative by health care professionals and industry to improve the way the computer systems in health care share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical need in support of optimal patient care.	Integrating the Healthcare Enterprise
Incident Commander	The officer in charge of the overall management of an incident at the incident site. He or she is responsible for building management organization based on a span of control and incident complexity. There is only one incident commander per incident.	Emergency Responder Use Case
Inpatient	A patient who is hospitalized to receive health care treatment.	Medication Management Use Case
Integrity	Proof that the message content has not been altered, deliberately or accidentally, in any way during transmission.	Adapted from ISO 7498-2:1989
Inventory Managers	Individuals, from public or private organizations, who are responsible for coordinating inventory resources to support the delivery of care. These individuals determine the needs and coordinate logistics (including interacting with suppliers and vendors) to support the delivery of care.	Immunization Use Case
Knowledge Providers	Associations of public health individuals/organizations who provide technical and clinical advice/guidance and assistance to state and local health agencies in a broad range of areas including: occupational health, chronic diseases, injury control, and maternal and child health.	Immunization Use Case
Manufacturers/ Distributors	Entities that may be involved in the following activities: research, development, testing, production, storage, distribution, surveillance, and communication regarding medical/health care products at the community, regional, and national level, such as pharmaceutical manufacturers, drug wholesalers, medical device suppliers, etc.	Immunization Use Case
Medical Examiner	A physician officially authorized by a governmental unit to ascertain the cause of death. Unlike a coroner, the medical examiner is always a physician.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Medication	Medication includes any prescription medications, sample medications, herbal remedies, over-the-counter drugs, vaccines, and diagnostic and contrast agents used on or administered to persons to diagnose, treat, or prevent disease or other abnormal conditions. This also includes any product designated by the FDA as a drug with the exception of eternal nutrient solutions, oxygen, and other medical gases.	Medication Management Use Case
Medication History	A list of past and present prescription and non-prescription patient medications that is relevant for future clinical episodes.	Medication Management Use Case
Medication List	A compilation of current medications. This may also include the history of medications for a period of time. A medication list includes medication start and stop dates, and may include the clinical indication.	Medication Management Use Case
Medication Management	The system for how health care organizations handle medications. The medication management process includes ordering and prescribing, preparing and dispensing, administration, monitoring, medication selection and procurement (i.e., formulary considerations), and medication storage.	Medication Management Use Case
Medication Network Intermediaries (MNIs)	These entities support the health care process by accomplishing communication among providers, pharmacies, and pharmacy benefits managers or payors as needed for medication dispensing and reimbursement. In this role, they are both a conduit for communication and a source of information on aspects of medication management such as medication prescription history, dispensing status, and pharmacy benefits. This stakeholder group includes Pharmacy Network Intermediaries, ePrescribing Network Intermediaries, clearinghouses, and similar organizations.	Medication Management Use Case
Medication Order	Traditionally handwritten or verbally communicated order for patient care, provided to the medical staff (nurses, therapists or other physicians) or to the departments (pharmacy, laboratory or radiology) responsible for fulfilling the order. A medication order can also be electronic.	Medication Management Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Medication Reconciliation	Formal process of obtaining a complete and accurate list of each consumer's current medications—including name, dosage, frequency and route—and allergies and documenting decisions that are made about which medications are continued as the patient transitions from one level or setting of care to another (admission to hospital, intra-hospital transfer, discharge to home). For patient transitions that transfer the patient from one setting to another (hospital to PCP or long-term care), medication reconciliation requires communication of information to the next provider of care and to the patient.	Medication Management Use Case
Modeling State	ASPC member states with a health information exchange infrastructure in operation or in the process of establishing exchanges. Each modeling state documented their system infrastructure and architecture to use with the use case approach to yield an optimized test environment for establishing a minimum policy.	ASPC Collaborative
MTF	Medical Treatment Facility. A facility established to provide medical treatment to patients including hospitals, urgent care centers, ambulatory care centers, and temporary medical facilities established for a large-scale emergency.	Emergency Responder Use Case
National Incident Management System (NIMS)	The NIMS integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity.	Emergency Responder Use Case
Network	An open communications medium, typically the Internet, that is used to transport messages between the Claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking) and passive (e.g., eavesdropping) attack at any point between the parties (Claimant, Verifier, CSP or Relying Party).	NIST 800-63-1

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
NHIN	The Nationwide Health Information Network is being developed to provide a secure, nationwide interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and health care.	The U.S. Department of Health and Human Services
NIST	The National Institute of Standards and Technology is a non-regulatory agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.	The National Institute of Standards and Technology
Non-Regulated Health Professional	Person employed by a health care organization who is not a regulated health professional. Examples: Medical receptionist who organizes appointments or a nurse's aide who assists with patient care. Note: The fact that a body independent of the employer does not authorize the employee's professional capacity does not, of course, imply that the employee is not professional in conducting her/his services.	[ISO IS17090]
Non-Repudiation	Service providing proof of the integrity and origin of data (both in an unforgeable relationship), which can be verified by any party.	Adapted from ASTM [31].
Object Identifier [OID]	A number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using a notation of digits and dots, OID resemble very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.	PC Encyclopedia
ONC	Office of the National Coordinator for Health Information Technology; serves as the Secretary's principal advisor on the development, application, and use of health information technology in an effort to improve the quality, safety, and efficiency of the nation's health through the development of an interoperable harmonized health information infrastructure.	Emergency Responder, Medication Management, Immunization Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
On-site Care Providers	On-site care providers are the initial personnel to deliver medical care at the scene of an incident. While this would typically be emergency medical technicians (EMTs), it can also include medically trained fire, law enforcement, and uniformed services medical personnel and civilian disaster medical assistance teams (DMATs).	Emergency Responder, Immunization Use Case
On-site Care Record	The on-site care record is used to collect information provided at the scene of the incident by on-site care providers. This is typically provided to ED staff and becomes a part of the patient's electronic health record. The on-site care record is currently known by other titles, such as 'Ambulance Run Report'.	Emergency Responder Use Case
OPHEP	HHS Office of Public Health Emergency Preparedness.	Emergency Responder Use Case
Organization Employee	Person employed by a health care organization or a supporting organization. EXAMPLES: Medical records transcriptionists, health care insurance claims adjudicator, and pharmaceutical order entry clerks.	[ISO 17090]
Organization Roles	Organizational roles correspond to the hierarchical organization in a company in terms of internal structures.	Neumann/Strembeck
OTC	Over-the-counter, as in OTC medication, which implies that it does not require prescribing by a physician.	Medication Management Use Case
Outpatient Medication List	Also known as the "home medication list," a list of current medications assembled at admission to an ED or hospital. It is assembled from the patient (or other patient representative) and from available external electronic sources and is intended to include all current prescribed medications, as well as OTC, herbal and homeopathic drugs, and dietary supplements the patient is taking.	Medication Management Use Case
Outpatient Pharmacies	Pharmacies that are primarily engaged in filling ambulatory patient prescriptions.	Medication Management Use Case
Password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.	NIST 800-63-1
Patient Identifier Cross-referencing (PIX)	Provides cross-referencing of patient identifiers from multiple Patient Identifier Domains. These patient identifiers can then be used by identity consumer systems to correlate information about a single patient from sources that know the patient by different identifiers.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 15)

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Patient Regulator	As used in the military services, those who determine where ambulances take patients. This term is also known in the non-military setting as Medical Control and/or EMS Director.	Emergency Responder Use Case
Patient/Consumer	Person who is the receiver of health related services and who is an actor in a health information system.	ASPC negotiated definition
Patients	Members of the public who receive health care services.	Immunization, Medication Management Use Case
Persistence	In computer science, persistence refers to the characteristic of data that outlives the execution of the program that created it. Without this capability, data only exists in RAM.	Programming persistence in chi Authors: Sajeev, A.S.M.; Hurst, A.J. Description: Computer Start Page: 57 End Page: 66 ISSN: 0018-9162 ISBN: Volume: 25 Issue: 9
Personal Health Record	An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.	National Alliance For Health Information Technology
Personal Health Record (PHR) System Suppliers	Organizations that provide specific PHR solutions to clinicians and patients such as software applications and software services. These suppliers may include developers, providers, resellers, operators, and others who may provide these or similar capabilities.	Immunization Use Case
Personal Identification Number (PIN)	A password consisting only of decimal digits.	NIST 800-63-1
Pharmacies	Organizations that dispense pharmaceuticals to consumers, utilize data to check for contraindications and allergies, and potentially participate as an intermediary or subnetwork provider of data on dispensed medications or provide PHR services.	Immunization Use Case
Pharmacists	Health professionals and clinicians who are licensed to prepare and dispense medication pursuant to the request of authorized prescribers. The practice of pharmacy includes, but is not limited to, the assessment, monitoring, and modification of medication and the compounding or dispensing of medication. Direct care activities that pharmacists can perform include patient education, patient assessment, and consultation.	Immunization, Medication Management Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Pharmacy Benefit Managers (PBMs)	These entities manage pharmacy benefits on behalf of payors, interacting with pharmacies and providers via a pharmacy network intermediary. As part of this role, they can provide information on pharmacy benefits available to an individual consumer and an individual consumer's medication history.	Medication Management Use Case
Pharmacy Systems	Electronic systems that support pharmacists with their role in dispensing medication. This includes systems that may be able to provide useful information on consumers' past medication histories.	Medication Management Use Case
Point-to-Point Exchange	A direct link or communication connection with defined endpoints.	Medication Management Use Case
Possession and Control of a Token	The ability to activate and use the token in an authentication protocol.	NIST 800-63-1
Prescription	An order made by a qualified health professional to a pharmacist or other therapist for the preparation and administration of a drug or device for a patient.	Medication Management
Privacy	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.	[ISO/IEC 2382-8:1998]
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.	NIST 800-63-1
Problem List	A synopsis of the patient's medical conditions, such as diabetes, hypertension, ankle fracture, etc.	Emergency Responder Use Case
Proof of Possession (PoP) protocol	A protocol where a Claimant proves to a Verifier that he/she possesses and controls a token (e.g., a key or password).	NIST 800-63-1
Providers	The health care clinicians within health care delivery organizations with direct patient interaction in the delivery of care, including physicians, nurses, psychologists, and other clinicians. This can also refer to health care delivery organizations.	Immunization Use Case
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.	NIST 800-63-1
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber identified in the certificate has sole control and access to the private key.	NIST 800-63-1

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Public and Private Immunology, Vaccine Response, and Adverse Event Experts	Governmental organizations, and physician associations that make decisions or recommendations on issues including: licensing vaccines, establishing effective and safe dosages, establishing schedules for vaccine administration based on immunology principles, pre- or post- exposure prophylactics, proper handling of vaccines, reporting of adverse events, and defining adequate documentation of vaccination events for coverage assessments and recall of patients or vaccine lots.	Immunization Use Case
Public and Private Sector Supply Chain	Entities involved in the production, storage, and distribution of medication and immunization products at the community, regional, and national level, such as pharmaceutical or vaccine manufacturers, drug and vaccine wholesalers/distributors, and pharmacies and retail delivery organizations.	Immunization Use Case
Public Health Agencies/ Organizations (federal/state/local/ territorial/tribal)	Federal, state, local, territorial, and tribal government organizations, and clinical care personnel that exist to help protect and improve the health of their respective constituents. These organizations are also involved in the coordination of ordering and distributing resources such as vaccines.	Immunization Use Case
Public Health Knowledge Providers	Associations of public health individuals/organizations who provide technical advice and assistance to state and local health agencies in a broad range of areas including: occupational health, infectious diseases, immunization, environmental health, chronic diseases, injury control, and maternal and child health.	Immunization Use Case
Public Health Systems	IT systems used by the various public health entities at the various levels of government (local, state, and federal). These systems are mostly used to perform the functions of biosurveillance and health trend monitoring.	Emergency Responder Use Case
Regional Health Information Organization	A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.	National Alliance For Health Information Technology
Registration	The process through which a party applies to become a Subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.	NIST 800-63-1

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Registration Authority (RA)	A trusted entity that establishes and vouches for the identity of a Subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).	NIST 800-63-1
Registries	Organized systems for the collection, storage, retrieval, analysis, and dissemination of information to support health needs. This also includes government agencies and professional associations, which define, develop, and support registries.	Immunization Use Case
Registry Stored Query	An ad-hoc query invoked by a transaction issued on behalf of a care provider to a Document Registry. A search of the registry locates documents that meet the provider's specified query criteria and returns registry metadata containing a list of document entries found to meet the specified criteria including the locations and identifier of each corresponding document in one or more Document Repositories.	IHE ITI-18
Regulated Health Professional	Person who is authorized by a nationally recognized body and qualified to perform certain health services. Examples: Physicians, registered nurses, and pharmacists. Note 1: The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations, and other formally and nationally recognized organizations. They may be exclusive or non-exclusive in their territory. NOTE 2: A nationally recognized body in this definition does not imply one nationally controlled system of professional registration but, in order to facilitate international communication, it would be preferable for one nationwide directory of recognized health professional registration bodies to exist.	[ISO IS17090]
Rehabilitative Care	After hospitalization, people who need continued inpatient skilled nursing care to ease the transition back to home are taken care of in rehabilitative care.	Emergency Responder Use Case
Repository	A repository providing a central storage location for electronic health records—provides aggregation point for information used by public health practitioners and emergency operations management.	Emergency Responder Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Resource Managers	Individuals who are responsible for coordinating resources to support the delivery of care. These individuals determine the needs and coordinate logistics to support the delivery of care.	Immunization Use Case
Response Management Organizations	Organizations that are responsible for emergency evaluation and response to natural disasters [e.g., public health and emergency management organizations (Federal Emergency Management Agency, Red Cross, etc.)].	Immunization Use Case
Role	Set of competences and/or performances that are associated with a task.	[ISO TS21298]
RTI	RTI International.	N/A
Schools	Organizations that provide education and can also serve in a public health support role. Educational facilities may have vaccination requirements for matriculation. In some instances, schools have are delegated to input vaccination status/history into data repositories such as Immunization Information Systems (IISs).	Immunization Use Case
Secure Node	The secure node is responsible for providing reasonable access controls. This typically includes user authentication and authorization. The secure node is also responsible for providing security audit logging to track security events. The difference between the Secure Node and the Secure Application is the extent to which the underlying operating system and other environment are secured. A Secure Node includes all aspects of user authentication, file system protections, and operating environment security. The Secure Application is a product that does not include the operating environment.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 64)
Security	Combination of availability, confidentiality, integrity, and accountability.	[ENV 13608-1]
Security Policy [primary—internal]	Plan or course of action adopted for providing computer security.	[ISO/IEC 2382-8:1998]
Security Policy [secondary—external]	Service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.	[ISO 7498-2:1989]
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.	NIST 800-63-1
Specialty Treatment	Medical treatment provided by providers or in institutions designed uniquely for specific types of treatment.	Emergency Responder Use Case
Signer	Entity generating a digital signature.	ISO/IEC 1st CD 13888-1: 2007-11-12

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Sponsored Health Care Provider	Health services provider who is not a regulated professional in the jurisdiction of his/her practice, but who is active in his/her health care community and sponsored by a regulated health care organization Examples: A drug and alcohol education officer who is working with a particular ethnic group, or a health care aid worker in a developing country.	[ISO IS17090]
Subscriber	A party who receives a credential or token from a CSP.	NIST 800-63-1
Structural Role	A structural role is a type of health care personnel warranting differing levels of access control. Also known as “basic role,” “organizational role,” or “role group.” For a listing of health care structural roles see ASTM E 1986-98 (e.g., Attending Physician)	ASTM E 1986-98
Supporting Organization	Officially registered organization that is providing services to a health care organization, but is not providing health care services. Examples: Health care financing bodies such as insurance institutions, suppliers of pharmaceuticals and other goods.	[ISO IS17090]
Symmetric Key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.	NIST 800-63-1
Temporary Care Facilities	Facilities set up temporarily to care for patients when the situation dictates that normal facilities cannot receive them.	Emergency Responder Use Case
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant’s identity.	NIST 800-63-1
Token Authenticator	The value that is provided to the protocol stack to prove that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.	NIST 800-63-1
Trading Partners	Entities that exchange (submit or receive) data electronically with each other. Examples include any pairing of physicians, providers, billing services, clearinghouses, health plans, or third-party administrators.	45 CFR 160.103 Trading Partner Agreements
Triage	The sorting of and allocation of treatment to disaster victims according to a system of priorities designed to maximize the number of survivors.	Emergency Responder Use Case Use Case

(continued)

Table C-1. ASPC Glossary and Abbreviations (continued)

Term	Definition	Source of Definition
Triage Collection Point	A temporary location, at or near an incident site, where patients who need medical care are situated until they can be transported to the ED or other appropriate medical care facility.	Emergency Responder Use Case
Verified Name	A Subscriber name that has been verified by identity proofing.	NIST 800-63-1
Verifier	An entity that verifies the Claimant's identity by verifying the Claimant's possession of a token using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the token and identity and check their status.	NIST 800-63-1
(XDS) Cross-Enterprise Document Sharing	Enables a number of health care delivery organizations belonging to an XDS Affinity Domain (e.g., a community of care) to cooperate in the care of a patient by sharing clinical records in the form of documents as they proceed with their patients' care delivery activities. This profile is based upon ebXML Registry standards, SOAP, HTTP and SMTP. It describes the configuration of an ebXML Registry in sufficient detail to support Cross Enterprise Document Sharing.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 16)
XDS Document	An XDS Document is the smallest unit of information that may be provided to a Document Repository and registered in a Document Registry. An XDS Document may contain simple text, formatted text (e.g., HL7 CDA Release 1), images (e.g., DICOM) or structured and vocabulary coded clinical information (e.g., CDA Release 2, CCR), or may be made up of a mixture of the above types of content.	Vol. 1 (ITI TF-1): Integration Profiles, Rev. 4.0 Final Text 2007-08-22 (p. 156)
(XUA) Cross-Enterprise User Assertion Profile	Provides a means to communicate claims about the identity of an authenticated principal (user, application, system) in transactions that cross-enterprise boundaries. To provide accountability in these cross-enterprise transactions, there is a need to identify the requesting principal in a way that the receiver can make access decisions and generate the proper audit entries. The XUA Profile supports enterprises that have chosen to have their own user directory with their own unique method of authenticating the users, as well as others that may have chosen to use a third party to perform the authentication.	[http://wiki.ihe.net/index.php?title=Cross-Enterprise_User_Assertion_Profile]
Zero-knowledge Password Protocol	A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the Verifier. Examples of such protocols are EKE, SPEKE and SRP.	NIST 800-63-1

APPENDIX D:
RESULTS FROM THE ENVIRONMENTAL SCAN FOR AUTHENTICATION AND AUDIT

The Environment Scan for Provider Authentication and Audit reviewed organizational policies and process in the following areas:

1. Health care provider *Use Agreement* content.
2. *Registration* of the provider to become a subscriber of the health information organization.
3. Process for *Verifying the Identity* of the provider.
4. *Identity Provisioning* of the provider.
5. Health information organization activities for *Maintenance* of health care provider system use.
6. *Access Control.*
7. *Audit.*

The ASPC summarized the information gathered from the state teams and limited stakeholders. The combined information then served to establish a baseline of current practices in the collaborative states.

Note: Because some questions allowed respondents to provide multiple answers, the totals for those questions will not add up to 100%.

1. Use Agreement

The respondents indicated that the following components should be required in a Use Agreement:

- Access and use of information will occur only as permitted under the agreement (97%).
- Information provided is true, accurate, and complete (87%).
- It is understood that there are penalties for failure to abide by the contract (78%).
- User promises to comply with present and future federal and state laws (74%).
- User promises to act in good faith and be truthful at all times (74%).

2. Registration

The following information was identified as being required when registering a provider:

First Name & Last Name **(73%)**, NPI **(55%),** DEA number **(55%),** Principal practice location **(55%),** Profession **(45%),** Specialty **(45%),** State License Number **(45%),** SSN

(36%), e-Mail address **(27%),** Legacy Number **(27%),** Date of Birth (**18%**), Home Address/phone **(18%),** and Taxonomy Code **(9%).**

The following registration information is retained by the respondents to verify their participant provider's identity:

Provider Information **(27%),** Address **(27%),** Name **(18%)**, DEA Number**(18%)**, State License Number **(18%)**, Date of Birth **(18%),** Principal Practice **(18%),** NPI **(9%)**, User ID **(9%)**, SSN **(9%)**, e-Mail Address **(9%)**, W9 **(9%)**, Disclosure **(9%)**, or Gender **(9%)**.

The minimum data set needed by the respondent organization to authenticate any individual using the system was:

Two data elements **(40%)**, Three data elements **(30%),** Four data elements **(10%),** Five data elements **(5%)**, Six data elements **(10%)** or Seven data elements **(5%).**

A minimum data set used by the respondent organization to authenticate any individual included the following elements:

User ID **(50%)**, Name **(35%)**, Password **(35%)**, Photo Id **(25%)**, SSN **(20%)**, DOB **(20%)**, Address **(15%)**, Face-to-face **(10%)**, KBA **(5%)**, NPI **(5%)**, DEA **(5%)**, State license number **(5%)**, Role **(5%)**, Principal Practice **(5%)**, Training Certification **(5%)**, User Agreement **(5%)**, Academic Credentials **(5%)**, Manager Authorization **(5%)**, Criminal Background Check **(5%)**, Trading Partner Number **(5%)**, Patient Access **(5%)**.

77% of responding organizations register users based on roles.

For the respondent organizations who register users based on roles, they manage the roles:

- By the site-specific administrator (13%).
- Roles are defined and managed by Active Directory and by application (6%).
- Roles are added/removed by system administrators (6%).
- Single access role for clinical or treatment and administrative roles without access to clinical data (6%).
- 220 different profiles for staff based on job code (6%).
- Health care entity defines roles and responsibility (6%).
- Roles are managed by registration step, based on organization affiliation and clinical entry access (6%).
- Registrant is recognized by the system as a physician provider or another type (6%).
- There is one role per person, even if acting in different roles (6%).
- One role only is used (6%).

- Roles are verified at initial login (6%).
- Roles are managed by policy from a governing body (6%).
- Roles are defined centrally and delegated (6%).
- Role is clinical provider, clinical staff, or clerical staff (6%).
- Role is managed by the type of provider (6%).

73% of respondents collect affiliation information on their users.

3. Verifying Identity

55% of respondents verify the credentials of their health care providers with a licensing database, when registering them to participate in their HIE or before disclosing PHI to providers.

55% of their providers are required to prove their identity in a face-to-face manner with a licensing authority, notary public, or some other form. The processes used to verify the identity of any user or entity accessing the respondent's system includes: Trusted Third Party **(48%),** Face-to-Face **(48%),** Knowledge-based Authentication **(30%),** Shared Secrets **(26%)**, Notary **(22%)**, or some other process **(30%).**

50% of the respondent's verification method depends on the type of user.

When connecting to another HIO, the reported acceptable/required process from a trading partner to verify the identity for users of their system would be: Trusted Third Party **(52%)**, Shared Secrets **(38%)**, Knowledge-based Authentication **(33%)**, Face-to-Face **(29%)**, Notary **(14%)**, or some other process **(24%).**

4. Identity Provisioning

86% of respondents use one factor authentication in their provisioning system. **14%** use two factor, and no respondents use three factor.

73% of the respondents have systems that allow on-site access. **91%** have systems that allow remote access.

96% of respondents provision each individual user with a separate and unique credential.

Respondents use the following for mechanisms for authentication: Password **(91%)**, PIN **(36%)**, One Time Password **(9%)**, Digital Certificate **(9%),** Biometrics **(9%)** or some other type **(9%)**. No respondents use Cryptographic Token, a Proximity Card, or Picture Recognition.

5. Maintenance

64% of responding organizations have an established time limit on provisioning of users.

55% of the responding organizations have both the user and the administrator as responsible for maintaining registration data, **40%** have just the administrator, and **5%** just the user.

73% of respondents force re-registration. Of those that force re-registration, **50%** indicated 262 days as the interval for re-registration, **25%** indicated 365 days, and **25%** indicated 1,095 days.

75% of respondents require re-verification of identity for re-registration. **25%** require re-registering of user identity attributes and no respondents require re-provisioning of users.

27% of renewals are based on application date, **18%** on calendar date, and **9%** on birth date. **45%** of respondents reported some other type of date not listed.

82% of respondents have a process for updating information about users.

The following information is maintained by respondents in their re-registration process: The same information as the initial registration **(55%)**, respondents only verify if existing information on file **(15%)**, no information is available or has yet to be determined **(15%)**, less information than the initial registration **(10%)**, or information is same as initial registration and respondents verify existing information **(5%)**.

The respondents reported that their systems:

- allow for enforcing the use of strong passwords **(82%);**
- allow for mapping to an individual **(64%);**
- support only allowing the user to use the same password only once every X iterations **(55%);**
- prohibit simultaneous access of the same user ID/concurrent connections **(55%)**; and
- support maintenance of multiple factor authentication **(36%).**

When asked in a multiple choice question to “select all that apply,” no respondent reported that their systems:

- allow for periodic forced password change,
- support one logon ID with multiple passwords to coordinate group access requirements,
- support automatic logoff or timeout, and
- use screensaver passwords.

When asked in separate questions for a “yes/no” answers regarding their systems:

86% of respondents indicated that their system allows for passwords to be forced to be changed periodically.

91% of respondents have their system support automatic logoff or timeout or screensaver passwords.

The respondents reported the following intervals for forcing passwords to be changed: 90 days **(61%)**, 0 days **(11%)**, 60 days **(11%)**, 120 days **(11%)**, 9,999 days **(6%)**.

64% of respondents have automatic logoff or timeout or screensavers installed and monitored.

82% of respondents reported that they have a suspension process. **82%** reported a process for revoking privileges for providers. **82%** reported having a mechanism by which access is terminated.

68% of respondent organizations provide the person who maintains the information with support, system, or manual prompts, which notifies or alerts when there are users needing renewal. The type of support provided includes: prompts manual or automatic **(67%)**, e-mail messages **(22%)**, or a report **(11%)**.

76% of respondents have a policy for terminating or suspending digital credentials. The access termination is completed and documented either: immediately upon notification **(63%)**, dependent on reason for termination **(9%)**, in 1 month **(18%)** or is not known to the respondent **(18%)**.

81% of respondents require documentation of access termination.

6. Access Control

The following pieces of information are passed between the authentication and the access control system of the respondents: a unique ID **(100%)**, role **(64%)**, affiliation **(41%)**, or authentication method **(36%)**.

The respondents reported that their process for authenticating a provider who is provisioned within their system and requesting access to patient health information requires: user name and password **(44%)**, general open access **(11%)**, some other process not listed **(44%)**. **64%** of respondents verify the authentication method of the provider requesting the information.

64% of respondents have the capability to ensure that the entities communicating with them are authenticated. **55%** have a procedure in place to identify the location of the user requesting the information.

The respondents reported that their systems:

- authenticate users to access the system based upon role (64%),

- authenticate communications (55%),
- accommodate data integrity checks (45%), and
- authenticate other systems without a user-specific authentication (36%).

The respondents allow system-level authentication to the following type of entities: hospitals **(70%)**, physician's groups/clinics **(70%)**, laboratories **(60%)**, pharmacies **(50%)**, state agencies **(40%)**, payers **(10%)**, or other entities not listed **(40%)**. **73%** of respondent organizations send the ID of the responsible individual or entity sender with the request.

64% of respondents have a unique identifier with each message. **64%** of respondents have the ID of the responsible receiver registered or logged.

64% of respondent organizations are currently using an open network to transmit PHI. **100%** reported using Data Encryption.

7. Audit

91% of respondent organizations have a designated, assigned, separate role for a Security Administrator. **100%** of respondents can identify every individual or entity that has access to the system.

100% of respondent organizations can identify when a user viewed those data, **96%** can identify who viewed what data, and **50%** can identify for how long (length of time) data were viewed.

80% of respondents can provide access to audit records for the patient whose data are being viewed.

The respondent organizations reported that they track: access violations within their system **(82%),** unsuccessful login attempts **(64%)**, transmission of PHI outside their system **(36%)**, and downloads of PHI **(27%)**.

91% of respondents reported security administrative functions are logged within their system, and **91%** reported that system administration functions are logged.

The respondents reported that their systems:

- generate audit logs that contain information specific to those who have accessed, created, modified, deleted, or transmitted the data (91%);
- back up audit logs (91%);
- have the ability to produce an alarm based on unauthorized access (82%);
- keep a log of user activity, including all access to networked system activity (82%);
- test for backup recovery (73%); and

- provide an alarm for unusual/inappropriate activities with volume thresholds (27%).

64% of respondent systems have the ability to produce an alarm based on unauthorized access. **57%** have an alarm installed that reports unauthorized access.

100% of respondents have audit records protected against unauthorized access, modifications, or deletion. **73%** of the organizations have defined audit record elements that are necessary to track.

91% of respondents' security administrators have the authority to request or generate audit log reports. The following information is captured in the audit logs: user identification **(91%)**, date and time of event **(82%)**, patient identification **(82%)**, identification of the patient data that are accessed **(82%)**, type of action taken **(64%)**, reason for access **(55%)**, source of access **(45%)**, a recognition that both an electronic "copy" operation and a paper "print" operation are qualitatively different from other actions **(36%)**, access device identity **(27%)**, or user demographics **(18%)**.

The respondents reported the following is captured for routine disclosures:

- date and time of disclosure (91%),
- identity of person requesting (91%),
- identity and verification of the party receiving the information (91%),
- identity of target about which data are being sent (82%),
- description of information disclosed (64%),
- reason for disclosure (45%),
- identity of the agent (individual or application) disclosing the information (45%),
- patient authorization tracking (specially protected health information/state and federal) (45%), and
- verification method of requesting the party's identity (18%).

The respondents reported the following is captured for legal disclosures:

- date and time of disclosure (91%),
- description of information disclosed (55%),
- identity and verification of the party receiving the information (55%),
- subpoena number, date, and issuer (could be court, attorney, or law enforcement) (46%),
- reason for disclosure (45%),
- verification method of requesting the party's identity (27%),
- court docket number (27%),

- names of the parties (27%),
- name and location of the court where proceeding is held (27%),
- verification that patient has been notified (if required) of the release (18%), and
- administrative proceedings (18%).

The respondents reported the following is captured for emergency disclosures:

- date and time of disclosure (64%),
- identity of patient (64%),
- identity of person requesting access (64%),
- identity and verification of the party receiving the information (64%),
- description of information disclosed (64%),
- description of circumstances that required emergency disclosure (45%),
- identity of the party disclosing the information (45%),
- case number (36%),
- identity of workforce member releasing information to public health as required (36%), and
- verification method of requesting party's identity (36%).

91% of respondents perform periodic reviews of generated audit logs.

82% of respondents have a comprehensive audit policy. Of these organizations, **100%** have formal audit criteria specified in the audit policy and **86%** specify the conducting of an annual evaluation or compliance audit.

50% of the respondents reported annual compliance audits conducted by an individual or group internal to the organization, **20%** by an individual or group external to the organization, and **40%** use a combination of the two.

90% of the respondent organization's audit findings are mitigated according to policy.

50% of respondent systems keep a log showing data transmission taking place for the purpose of data recovery. **60%** of systems keep a log that allows the organization to trace different types of data transmissions.

APPENDIX E:
SECURITY POLICY TEMPLATE

Authentication

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
1. Use Agreement	In the registration process, typically, the Registering Authority (RA) maintains records of the registration of subscribers. The registration and identity proofing process is designed, to a greater or lesser degree depending on the assurance level [i.e., *how "assured" the organization needs to be of the identity of the individual wanting access to their system*] to ensure that the RA knows the true identity of the Applicant. Specifically, the requirements may include measures to ensure that: 1. A person with the Applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person; 2. The Applicant whose token is registered is in fact the person who is entitled to the identity; 3. The Applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the Subscriber's token, the Subscriber cannot successfully deny he or she registered that token. However, the processes and mechanisms available to the RA for identity proofing may differ across organizations. (*excerpt adapted from NIST 800-63-1*)	—	—
a. Components	—	—	—
b. Administration	—	—	—
c. Validation of elements	—	—	—

(continued)

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
2. Identity Registration	"Registration Agreement" means a legally binding agreement between a sub-network organization [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. If the SNO does not wish to obtain Registration Agreements from Participants, this section should be omitted. "Services" means the information-sharing and aggregation services and/or software.	—	—
a. Required data set for authentication	—	P5: Authentication requires an identifier, and is required for authorization. Authentication is a way of allowing a user to prove that he is who he claims to be. The simplest form of authentication is in the providing of an identifying token, plus a secret of some sort, such as a bank card + PIN, or a username + password or phrase.	—
i. Credential verification	—	—	—
ii. Registration data persistence	—	—	—
b. Role-based registration	—	P5: All users must be authenticated before they are given access to any sub network organization-wide resource containing patient data. The local institution can ask users to log in and communicate the authenticated identifiers to other participants in the HIO (this is transitive trust) or the HIO can run authentication services itself, getting lists of users and roles from the participating institutions.	—

(continued)

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
c. User affiliations	—	—	—
3. Verifying Identity	A verified name is associated with the identity of a real person and before an applicant can receive credentials or register a token (i.e., password, smart card, or other token) associated with a verified name, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called *identity proofing*. The party to be authenticated is called a *Claimant* and the party verifying that identity is called a *Verifier*. When a *Claimant* successfully demonstrates possession and control of a token in an online authentication to a *Verifier* through an *authentication protocol*, the Verifier can verify that the Claimant is the Subscriber. The Verifier passes on an assertion about the identity of the Subscriber to the Relying Party. That assertion includes identity information about a Subscriber, such as the Subscriber name, an identifier assigned at registration, or other Subscriber attributes that were verified in the registration process. Authentication simply establishes identity, or in some cases verified personal attributes (for example the Subscriber is a US citizen, is a student at a particular university, or is assigned a particular number or code by an agency or organization), not what that identity is authorized to do or what access privileges he or she has; this is a separate decision. (*excerpt adapted from NIST 800-63-1*).	P5: Identity is an individual person or institution that needs access to health care data, for any purpose. Crucially, an identity is not merely a role; if you want to know the identity of someone who authorized a particular prescription, you want to know it was Dr. Smith, not just that it was a doctor.	—
a. Processes used to verify identity	—	—	—
b. Variations based on type and location of user	—	—	—
c. Accommodations for cross-HIE verification	—	—	—

(continued)

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
4. Identity Provisioning	Subscribers are registered and given a token. The token is used in an authentication protocol to bind that token to the identity, or to bind the identity to some other useful verified attribute. A Subscriber may be given electronic credentials (digital signature) to go with the token at the time of registration, or credentials may be generated later as needed. Authenticating subscribers requires a mechanism to uniquely identify each Subscriber and the associated tokens and credentials issued to that Subscriber. Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are: *Something you know (i.e., password and PIN—but note that if the provisioning includes both of these it is still single factor as these are both the same category / type of factor);* *Something you have (i.e., in your possession like a smart card or ID); or* *Something you are (biometrics).* *(excerpt adapted from NIST 800-63-1)* **Authentication systems may be one, two, or three factor.** *One factor* uses one of the three factors to achieve authentication. For example something you know like a password and PIN, **or** it may be something you have in your possession like a smart card. *Two factor* uses two of three factors to achieve authentication. For example, something you know **and** something you have like a private key on a smart card that is activated via PIN is a multifactor token. The PIN is something you know and the smart card is something you have. *Three factor* uses all three to achieve authentication. For example, something you know **and** something you have **and** something you are like a private key on a smart card that is activated via PIN and biometric read of a thumbprint. The PIN is something you know, the smart card is something you have, and the thumbprint is something you are.	—	—

(continued)

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
a. Types and levels of factor provisioning	Provisioning = The process of providing users with access to data and technology resources—this applies to authentication.	—	—
b. Individual versus organizational credentials	Credentialing refers to "electronic credential" i.e., digital signature.	—	—
5. Identity Maintenance	Token and credential management activities may include storage, renewal /reissuance, revocation and destruction, and retaining records. Policies for renewal and reissuance of tokens and credentials may establish a time period prior to the expiration of the credential, when the Subscriber can request renewal or reissuance following successful authentication using his or her existing, unexpired token and credential. For example, a digital certificate may be renewed for another year prior to the expiry of the current certificate by proving possession of the existing token (i.e., the private key). However the Subscriber may be required to reestablish his or her identity once the Subscriber's credentials have expired. Certain types of tokens may need to be explicitly deleted or zeroized at the end of the credential life in order to permanently disable the token and prevent its unauthorized reuse. In addition maintenance policies may include maintaining a record of the registration, history, and status of each token and credential, including revocation. *(excerpt adapted from NIST 800-63-1)*	—	—
a. Registration data	—	—	—
i. Type of data maintained	—	—	—
ii. Responsibility for maintenance (new users, terminated users, changes to current users)	—	—	—

(continued)

Table E-1. An Assessment of Key Components—Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	Related Definitions and Examples	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
b. Re-registration	—	—	—
i. Forced timeframes	—	—	—
ii. Information validity at re-registration	—	—	—
c. Password maintenance (revoke, lost, forgotten, forced timeframe for changing)	—	—	—
d. Automatic Logoff	—	—	—
e. Simultaneous Login	—	—	—
f. Delegated maintenance functions	—	—	—
g. Termination policies and procedures	—	—	—

Audit

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7)

Recommendations put forth in the Connecting for Health Framework Policy 7 Auditing Access to and Use of a Health Information Exchange are designed around the use of a record locator service (RLS). The P7 assumes HIOs are sophisticated entities operating at a scale that is consistent with rigorous audit and other security practices.

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
6. Audit and Access Control as it applies to Audit	Trading partners may use a Subscriber's authenticated identity and other factors to make access control or authorization decisions. In any authenticated online transaction, the Verifier must verify that the Claimant [an individual whose identity is to be verified] has possession and control of the token that verifies his or her identity. A Claimant authenticates his or her identity to a Verifier by the use of a token and an authentication protocol. This is called *Proof of Possession (PoP)*. The object created by the Verifier to convey the result of the authentication protocol run is called an assertion. Assertions contain, at a minimum, the name, of the Claimant, as well as identifying information that permits recovery of registration records. A Relying Party trusts an assertion based on the source, the time of creation, and attributes associated with the Claimant *(excerpt adapted from NIST 800-63-1).*	—	—
a. Institutions have unique and persistent institution identifiers	Persistent = Existing or remaining in the same state for an indefinitely long time	P5: A sub-network (HIO) organization must have identifiers for all its participating institutions. The identifiers can be issued by the HIO or they can be adopted from an external source as long as that source guarantees the uniqueness and persistence of any identifier.	—
b. Users have unique and persistent user identifiers	Persistent = Existing or remaining in the same state for an indefinitely long time	—	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
c. Authentication occurs before access to any sub-network organization (SNO) resource containing patient data	A sub-network organization (SNO) operates as a health information data exchange organization (whether regional or 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"	P5: All users must be authenticated before they are given access to any HIO-wide resource containing patient data	—
d. Requests for data from an institution other than the user's log-in institution provides:	—	P5: Any request for data from a remote institution, an institution other than the one the user is logged in to must be accompanied by at least two pieces of identifying information, which institution authenticated the requesting user, and an identifier for that user. The institution should know where the request came from and who authorized it.	—
i. Which institution authenticated the requesting user	—	P5: Any request for data from a remote institution, an institution other than the one the user is logged in to must be accompanied by at least two pieces of identifying information, which institution authenticated the requesting user, and an identifier for that user. The institution should know where the request came from and who authorized it.	—
ii. The user's identifier	—	P5: Any request for data from a remote institution, an institution other than the one the user is logged in to must be accompanied by at least two pieces of identifying information, which institution authenticated the requesting user, and an identifier for that user. The institution should know where the request came from and who authorized it.	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
e. For an authorization failure event (Break the Glass), system access is accompanied by:	—	P5: Access failure for someone who should be authorized can happen "Break the Glass" for a number of situations: he or she does not remember the required information, emergency, other. Any request that allows a known user to request data they believe they need, e.g., physician attempting to access medication history of a patient, when the system would not otherwise give the person access, should be accompanied by a brief description of the rationale for the request.	—
i. A brief description of the rationale for the request	—	P5: Access failure for someone who should be authorized can happen "Break the Glass" for a number of situations: he or she does not remember the required information, emergency, other. Any request that allows a known user to request data they believe they need, e.g., physician attempting to access medication history of a patient, when the system would not otherwise give the person access, should be accompanied by a brief description of the rationale for the request.	—
ii. An identifier for the user	—	P5: No matter what the cause of the authorization failure in the Break the Glass scenario, any system access must be accompanied by an identifier for that user. In no case is an otherwise unidentified "Emergency" account to be used, on the grounds that it amounts to provisioning a role without an accompanying person identifier.	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
iii. Enhanced auditing	—	P5: Any request that allows a known user to request data they believe they need, when the system would otherwise not give them access, must be accompanied by enhanced auditing and timely human review.	—
iv. Timely review	—	P5: Any request that allows a known user to request data they believe they need, when the system would otherwise not give them access, must be accompanied by enhanced auditing and timely human review.	—
f. Logging and audit controls	—	P7: Recommends logging and audit control functions as a part of a comprehensive compliance program	—
i. VIP Records are Audited	VIP Records (Very Important People) have additional monitoring to ensure protection and reduce the risk associated with these records.	P7: Recommends audit of VIP records as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
ii. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches are	—	P7: Recommends procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
1. Developed and documented	—	—	—
2. Being followed	—	—	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
iii. Network intrusion detection system activity logs are reviewed	—	P7: Recommends network intrusion detection system activity logs as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
iv. System administrator authorizations and activity are reviewed	—	P7: Recommends review of system administrator authorizations and activity as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
v. Physical access to data centers is reviewed	—	P7: Recommends review of physical access to data centers as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
vi. Technical, physical and administrative safeguards established by the policies of the organization are reviewed	—	P7: Recommends review of other technical, physical, and administrative safeguards established by the policies of the organization as part of compliance in addition to random audits of demographic and clinical records based on the level of risk for that portion of the system.	—
g. Periodic internal audits to evaluate process and procedures intended to secure protected health information (PHI) are conducted	—	—	—
i. Appropriate security practices, policies, and procedures are properly documented	—	—	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
ii. Those practices, policies, and procedures are implemented	—	—	—
iii. Practices, policies, and procedures meet the requirements of the HIPAA security rule	—	—	—
iv. Appropriate administrative physical and technical safeguards protect both electronic and nonelectronic PHI records	—	—	—
h. Information Access	—	—	—
i. Need to know/ minimum necessary for data management and release is established	—	—	—
ii. Need-to-know procedure/process for personnel access to PHI is established	—	—	—
i. System Capabilities	—	—	—
i. Users' system login and logoff is logged with date and time, or an external security system records the access	—	P7: The system is required to log user's system login and logoff with dates and time, or, if the system does not have the capability to record logon/logoff activity, it may rely on an external security system access control logging function to record access.	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
ii. The system can log read, create, update, delete, forward and print access initiated by individuals and process for systems containing confidential and restricted data	CCR = Continuity of Care Record, an ANSI-accredited health information technology standard. Its purpose is to make it possible for a digital summary of relevant administrative and clinical health information about an individual to be created, stored, and passed from one computer system to another.	P7: The system must have the ability to log, read, create, update, delete, forward, and print access initiated by individuals and processes for systems containing confidential and restricted data. For data warehouses, data marts, and operational data stores, the system must have the ability to log queries, or alternatively the tables read must be logged. Row-level logging must be available on demand.	—
iii. Audit records are identified by a unique record key or number and include	—	P7: All audit records must be identified by a unique record key number and include the following listed below:	—
1. User identifier/ name of user	—	P7: continued- User identifier/name of user	—
2. Time/date	—	P7: continued- Time/date	—
3. Device identifier (when used to access)	—	P7: continued- Device identifier (when used to access)	—
4. Source (i.e., subsystem or system of origin of the access request)	—	P7: continued- Source (i.e., subsystem or system of origin of the event [access request])	—
5. Content (type of data being accessed or activity being performed)	—	P7: continued- Content (type of data being accessed or activity being performed)	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
6. Type of action (e.g., read, write, update, delete, or copy) or access for diagnostic purposes	—	P7: continued- Type of action (e.g., read, write, update, delete, or copy) or access for diagnostic purposes. End.	—
iv. Unsuccessful login attempts and access violations within the system are logged	—	P7: Unsuccessful login attempts and access violations within the system must be logged	—
v. Unusual activity is logged	—	—	—
1. Multiple concurrent logins	—	—	—
2. Unauthorized access alarms	—	—	—
3. Volume thresholds	—	—	—
vi. Security administrative functions are logged	—	P7: Security administrative functions must be logged.	—
vii. Audit records are protected against unauthorized access, modifications, and deletion	—	P7: Audit records must be protected against unauthorized access, modifications, and deletion	—

(continued)

Table E-2. An Assessment of Key Components—Markle Foundation Connecting For Health Common Framework, Provider Authentication and Audit (P5 & P7) (continued)

ASC Policy Category	NIST Standards	Connecting For Health Recommended Policy Guidelines	Recommended Basic Minimum Requirements
viii. Audit records are readily available for 90 days and archived for a minimum of 2 years, or up to the 6 years used for the archiving of HIPAA disclosures	—	P7: Audit records must be readily available for 90 days and archived for a minimum of 2 years, or up to the 6 years used for the archiving of HIPAA disclosures	—
ix. Security administrators and auditors can request or generate reports that may consist of any or all of the audit record elements for any or all types of actions.	—	P7: Security administrators and auditors can request or generate reports that may consist of any or all of the audit record elements for any or all types of actions.	—

APPENDIX H:
UNIFORM SECURITY POLICY

Uniform Security Policy

March 31, 2009

TABLE OF CONTENTS

Introduction

Purpose. The purpose of the following authentication and audit minimum policy requirements is to foster cross-state and cross-model data exchange. This policy is intended to be agnostic to the state-specific health information exchange model(s) and is recommended by the HISPC Adoption of Standards Policy Collaborative (ASPC) as a set of basic, minimum policy requirements that have been publicly vetted and accepted. Through consensus negotiations between six states[5] and facilitation/support with the other ASPC states,[6] the ASPC has established baseline privacy and security protections for organizations engaged in exchanging electronic health information. Health information organizations (HIO) participating in health information exchange (HIE) may have different policies, but should incorporate these basic policy requirements for registering and authenticating users, both individual users and organizations, wishing to participate. The HIO must (1) register, (2) execute an agreement with, (3) verify the identity of, (4) provide digital identification for, and (5) maintain an account for all users. Each of these processes has a set of minimal requirements that must be defined or the participants of the HIO to trust their trading partners and users. The HIO must implement procedures for auditing access in HIE to confirm appropriate use. Pursuant to the American Reinvestment and Recovery Act, 2009 Title 13 Subpart D, the HIO and its business associates must submit to the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Scope. The scope of this policy is limited and specific only to electronic authentication and audit policies and process when a health care provider requests patient health information through an HIO for the purpose of treatment. The component parts included in this policy represent the requirements agreed to by participating states. The full scope of the requirements considered for negotiation is available in the ASPC full report at http://www.okhca.org/providers.aspx?id=10202.

Draft. March 27, 2009

How To Use. This policy does not serve as a standalone document. For more information on the HISPC project, go to: http://www.hhs.gov/healthit/privacy/execsum.htm.

Disclaimer. This policy has not been fully tested and is not intended to represent a complete security policy for health information exchange. This work is intended as a general resource (or reference) and is not meant to provide legal advice to any person or entity that receives a copy of the work. Readers should consult with competent counsel to determine applicable legal requirements, as well as privacy and security experts. Upon publication/public release of this document, please contact the Office of the National

[5] Arizona, Connecticut, Colorado, Nebraska, Oklahoma, and Washington.
[6] Maryland, Ohio, Utah, and Virginia.

Coordinator (ONC) for Health Information Technology, Health and Human Services (HHS) for additional information. E-mail: onc.request@hhs.gov.

Publication Version Control

Version	Date	Name	Purpose of Revision
Original	Jan 26, 2009	Chris Doucette Francesca Lanier	Initial Draft
Version 1.0	Feb 5, 2009	Chris Doucette	Add ASPC states / Legal / TAP comments
Version 2.0	Feb 25, 2009	Chris Doucette Francesca Lanier	Add Stakeholder Review Comments
Version 3.0	March 10, 2009	Chris Doucette Francesca Lanier	Add final Legal comments / Final Draft submittal to ONC.
Version 4.0	March 27, 2009	Chris Doucette Francesca Lanier	Final ASPC project deliverable

Authentication Policy

Section 1—Use Agreement

1.1 Requirement—Use Agreement

Health Information Organizations should have a data sharing agreement with participating providers that defines the privacy and security obligations of the parties participating in the HIO. These agreements should require the use of appropriate authentication methods for users of the HIO that depend on the user's method of connection and the sensitivity of the data that will be exchanged. In addition, these agreements should reasonably ensure sufficient auditing requirements to determine access and use of the system, and secure transport of health information across the network, are appropriate.

Where there is cross-HIO exchange of data, authentication and audit requirements should be defined through a Data Use and Reciprocal Support Agreement (DURSA). The DURSA should define the relationship between the HIOs and ensure, among other things, appropriate authentication and audit of users and queries across HIOs.[7] Reference: M2: A Model Contract for Health Information Exchange and P2: Model Privacy Policies and Procedures for HIE.

[7] Markle Foundation – Connecting for Health—http://www.connectingforhealth.org/.

Section 2—Identity Registration

2.0 Required Data Set for Authentication

A directory of data sources within the HIO will include primary contact information of registered members, identity attributes of providers, organization, and systems.

2.1.1 Data Source

A directory of data sources within the target HIO is required, and includes name of the HIO and any data sources within that HIO. The primary contact information for the data in the directories should include primary contact name and any contact phone numbers. *DAT 2*[8]

DAT 2 Attribute also considered:
Service location

2.1.2 Provider Identity Attributes

The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO.[9] Required elements are profession, role, name, the practice address (not home address), identity service provider and organization affiliation, business/legal address, and License/ID. Other attributes that are required, if they exist for this individual, include:

- Specialization/specialty,
- E-mail address,
- National Provider Identifier (NPI), and
- Digital identity. *DAT 10*

DAT 10 Requirements also considered:
Directory of all HIOs
Included in the directory: Contact fax numbers
Master provider index to query by provider for a specific patient

2.1.3 Organization Identity Attributes

Identifying the organization requires collecting the following attributes: organization name and e-mail address. Other attributes are required if they exist, including:

- Digital identity,
- EDI administrative contact,

[8] AUT *, AUD *, DAT *, SYS *, POL *—refers to a negotiated minimum policy requirement and can be referenced the Cross State technical source document.

[9] 45 C.F.R. § 164.312(a)(2)(i) (requiring assignment of a unique name or number for identifying and tracking user identity).

- Clinical information contact,
- Service Location, and
- Predecessor name and date of change.

If the HIO is a regulated health care organization, all supporting organization attributes above are required, as well as:

- License/ID,
- License status,
- Registered name, and
- Registered address. *DAT 11*

DAT 11 Attributes also considered:
Identifying an organization requires -License status

If the HIO is a regulated health care organization-Address
NPI
Organization address, National Provider Identifier (NPI), organization affiliation, closure date, and successor name

2.1.4 Identity Attributes of the Data Source System

Identifying the system requires the attributes of:

- System name,
- Digital identity,
- Organization affiliation,
- System IP address, and
- System domain name.

If there is no system domain name, the system IP address may be used. For purposes of identifying the originating electronic data sources, would require a date stamp and at least one of the following is required: the system (1) name, (2) IP address, or (3) domain name. Any identifying system types, such as the laboratory information systems, electronic health record system, emergency medical system, etc. should also be included. *DAT 12*

2.2 Role-based Access

Proper registration requires the establishment of a defined role associated with the registered user.

2.2.1 Role

The individual's organization role[10] is required for role-based access and should include the context of the organization. If the health care functional role[11] or the structural roles[12] exists, they are also required. *DAT 1*

[10] As defined in the American Health Information Community (AHIC) Use Cases.

Section 3—Verifying Identity

3.1 Processes Used to Verify Identity

Identity is verified through authentication of the user, the organization and the HIO's system.[13]

3.1.1 User Authentication

The methods for user identity vetting include both verifying the identity in person by a trusted authority and verification through the use of a demonstrated government-issued ID. The trusted authority is recognized by the state or federal government.

An applicant requesting an identity tied to a regulated provider type must have provider licensure validation. It is acceptable that this occur along with the validation required of any employee of a licensed provider organization.

Also, the HIO use of a specific naming convention as a primary identifier is required with a minimum assurance level used of Medium (knowledge/strong password/shared secret). *AUT 1*

AUT 1 Requirements also considered:

The use of a Notary for user identity vetting;
HIO using of an Object Identifier (OID) as a specific naming convention for the primary identifier;
The User handling sensitive information, given the state's legal/regulatory restrictions on records including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information

3.1.2 Organization Authentication

Organization identity vetting can be accomplished through personal knowledge of a registration authority, that the organization is who is says it is by a demonstrated documentation of corporate existence.

The HIO is required to use a specific naming convention as a primary identifier, and this would include the use of object identifier (OID) or idiosyncratic naming, if either of these exists. This is a requirement at the state level and the ASP Collaborative recommends development of a naming convention that can be registered and identified nationally.

The minimum assurance level required for organization authentication is High (PKI/Digital ID). *AUT 5*

---

[11] The functional role is dynamic and is a function of the role in which you are acting.
[12] A structural role is persistent and can be mapped to professions that are recognized.
[13] 45 C.F.R. § 164.312(d) (requiring "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed").

AUT 5 Requirements also considered:

Organization identity vetting using a certification such as Joint Commission, SAS-70 Compliance, or ENHAC Compliance
The Organization handling sensitive information, given the state's legal/regulatory restrictions information including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information.

3.1.3 System Authentication

System identity vetting, ensuring the data are coming from the system that they are supposed to be coming from, requires the assertion by an authorized organization representative and/or the demonstration of association with another licensed organization.

The minimum assurance level required for system authentication is High (PKI/Digital ID). *AUT 3*

AUT 3 Requirements also considered:

System identity vetting through in-person site visits, certification such as FDA or CCHIT, or verifying the system IP address and system domain name
The System handling sensitive information, given the state's legal/regulatory restrictions information including HIV, mental health, substance abuse, sexual health, prison health and/or genetic information.

3.2 Variations Based On Type and Location of User

3.2.1 User Identity, Role, and Affiliation Verification

The user identity, role, and affiliation must be checked for both revocation and expiration at the time of logon to the system. If either case pertains, use would be denied. *SYS 13*

SYS 13 Requirements considered as optional:

Authentication method checking and challenge/response checking

3.2.2 Signature Verification

The HIO is responsible for digital verification of nonrepudiation signer credentials. Verification implies that:

- The credential is issued by a trusted authority,
- The credential is current,
- The credential is not suspended or revoked, and
- The credential type is appropriate (for example, physician or pharmacist).

If the signed-by-person claimed (nonrepudiation) exists, it should also be verified. *SYS 11*

3.2.3 Assurance Level

It is required that the level of assurance be declared and should be communicated in terms of the then current National Institute of Testing and Standards (NIST) requirements. For the HIO to migrate data an assurance level of at least Medium (knowledge/strong password/shared secret) is required. *DAT 3*

3.2.4 Relationship To Patient

If the HIO is exchanging for purposes of treatment, the provider seeking access needs to demonstrate or certify that they have a treatment relationship with the patient. *POL 12*

POL 12 Requirement also considered:
A system ability to calculate some value that represents the quality of a match based on an algorithm, for purposes of tracking measurements

3.2.5 Threshold Calculation

Patient matching content out of scope.[14] *SYS 5*

3.2.6 Digital Signature

The HIO is required to have the ability to use digital signatures, if they exist, at least at the provider level. *SYS 9*

SYS 9 Requirement also considered:

A policy allowing the organization to accept or express data without signature or would it express with a caveat or some marker that no signature was received

[14] This requirement is outside the limited scope of the ASPC effort; however, the states elected to collect this information because of the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.

3.2.7 Persistence

The use of persistence[15] of the source signature is required and is the responsibility of the HIO with its own participants. The attributes required are persistent user signature, persistent organization signature, and persistent system signature. Nonrepudiation of origin is also the responsibility of the HIO with its own participants, and includes the attributes of user, organization, and system accountability. If source authentication exists it is also required. *DAT 8*

3.3 Accommodations for Cross-HIE Verification and Data Integrity

3.3.1 Restricted Data Sharing and Data Integrity

The transmission of caveats regarding data completeness is required to indicate that an entire record may not have been transmitted. The use of pertinent state-specific caveats should be included in the transmission. *POL 2*

3.3.2 Authenticate Recipient Identity (Organization / System / User)

The identity of the recipient must be established and the method of identifying recipients of communications can include, but is not restricted to (1) derived from ordering system communications, (2) selected from a provider directory, or (3) derived from identifiers included in the request for information. *AUT 6*

3.3.3. Required Elements for Matching

Elements for patient matching are considered out of scope,[16] including if patient matching is necessary for the authentication or audit functionality. *DAT 6*

DAT 6 Elements considered for patient matching include: Identifiers (Patient Account Number, SSN, Driver License, Mother's ID, MRN, Alt Patient ID); Patient Name (First, Middle, Last, Family Name, Suffix, Prefix/Title, Type); Mother's Maiden Name (Family Name, Surname); Patient DOB; Gender, Patient Previous Name; Race; Patient Home Address (Home Street, Street or mailing Address, Street Name, Dwelling Number, Other Designation (second line of street address), City, State/Province, Zip, Country, Address type, County Code); Patient Daytime Phone (country code, Area/City Code, Local Number, Extension, any other text); Work Telephone; Primary Language; Marital Status; Religion; Patient Ethnicity; Birth Place; Multiple Birth Indicator; Birth Order; Citizenship; Veteran's Military Status; Nationality; Deceased (Date/Time, Deceased Indicator)

[15] Persistence indicates proof that data have not been altered and are only valid during the communication session.

[16] This requirement is outside the limited scope of the ASPC effort; however, the states elected to collect this information due to the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.

3.3.4 Matching Criteria

Patient matching criteria is considered out of scope,[17] including if patient matching is necessary for the authentication or audit functionality. *DAT 7*

DAT 7 Requirement also considered:

Defining a minimum number of three (3) data elements to query another system

3.3.5 Digital Signature

For the purposes of cross-HIE verification, the ability to use digital signatures is required at the provider level. *SYS 9*

3.3.6 Persistence

The use of persistence of the source signature is required and is the responsibility of the HIO with its own participants. The attributes required are:

- Persistent user signature,
- Persistent organization signature and,
- Persistent system signature.

Nonrepudiation of origin is also the responsibility of the HIO with its own participants, and includes the attributes of:

- User Accountability,
- Organization Accountability, and
- System accountability.

If source authentication exists, it is also required. *DAT 8*

3.3.7 Data Authentication

For purposes of data authentication, the use of a timestamp is required at point of signature application. *AUT 4*

AUT 4 Requirement also considered, but is difficult to implement:

Signature Purpose (ASTM E1762)

3.3.8 Data Validation

Data validation of signer credentials should be issued by a trusted authority, should be current, and the credential should not be suspended or revoked and the credential

[17] This requirement is outside the limited scope of the ASPC effort; however, the states elected to collect this information due to the subject matter and relevancy as it related to the selected use cases. For more information see the ASPC Individual Requirements Review (IRR) document.

type should be appropriate (for example, physician, pharmacist or hospital). For purposes of data integrity, the data validation should indicate that the data have not been changed since the signature, and should have a timestamp at point of signature application. *AUT 7*

3.3.9 Type of Requestor

For verification purposes the requestor type should identify the exchange, organization (institution), and user (individual). *DAT 4*

3.3.10 Signature Purpose

The signature purpose should be included as a minimum requirement, and any of the captured signature elements that exist should be included. *DAT 13*

> *The DAT 13 elements that were considered include:*
>
> *Author's signature, Coauthor's signature, Co-participant's signature, Transcriptionist/Recorder, Verification signature, Validation signature, Consent signature, Witness signature, Event witness signature, Identity witness signature such as a Notary, Consent witness signature, Interpreter, Review signature, Source signature, Addendum signature, Administrative, Timestamp, Modification, Authorization, Transformation and Recipient*

Section 4—Identity Provisioning

4.1 Types and Levels of Factor Provisioning

Refer to Section 3 for the required assurance levels for user, organization, and system authentication [HISPC ASP reference AUT 1, 5 & 3 respectively].

Section 5—Identity Maintenance

5.1 Registration Data

No current minimum policy requirements exist.

Audit Policy

Section 1—Logging and Audit Controls

1.1 Log-In Monitoring[18]

As a part of log-in monitoring, an audit log is required to be created to record when a person logs on to the network or a software application of the HIO. This includes all attempted and failed logons.

The generated audit logs must be reviewed on a regular basis that is based on an audit criteria developed in advance. Anomalies must be documented and appropriate mitigating action and documented. The HIO should determine how long its state laws and risk management policies would require retention of this documentation. *POL 16*

1.2 Information Systems Review[19]

All HIE systems must be configured to create audit logs that track activities involving electronic Protected Health Information (PHI). The review of information systems shall include software applications, network servers, firewalls, and other network hardware and software. The generated audit logs shall be reviewed on a regular basis based on audit criteria developed in advance. All anomalies must be documented and appropriate mitigating action taken and documented. All system logs must be reviewed. The review shall include, but not limited to, the following types of information: data modification, creation, and deletion. The HIO should determine how long its state laws and risk management policies would require retention of this documentation *POL 15*

1.3 System Review

Information system reviews should be conducted on a regular and periodic basis, as determined by the HIO. *SYS 4*

SYS 4 Requirement also considered:

Automatic trigger exists for any out of state access; Automated Audit review to permit ready review of any interstate access exists

1.4 Security Audit Practice

The frequency of performing regular security audits shall be determined at a specified frequency for the HIO. Auditing frequency typically varies by state/HIO for example Nebraska conducts audits yearly, and Washington conducts quarterly

[18] HIPAA Security Rule: 45 C.F.R. § 164.312(b) (requiring "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"); 45 CFR § 164.308 (a)(5)(ii)(C) (requiring procedures for monitoring log-in attempts and reporting discrepancies).

[19] HIPAA Security Rule 45 CFR § 164.308 (a)(1)(ii)(D) (requiring covered entity to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports").

audits. Audits shall be conducted at least annually as a minimum requirement, and the comprehensive audit procedures should be developed, documented, and available. The HIO should also conduct periodic external audits. *SYS 8*

SYS 8 Requirement also considered:

The sharing of risk scores with other RHIOs

1.5 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication Integration Profile[20] requires the use of bidirectional certificate-based node authentication for connections to and from each node. The use of certificates or encryption is required when the data are signed or when it is specified by the HIO policy. *SYS 6*

Section 2—Periodic Internal Compliance Audits

To appropriately ensure the security of Protected Health Information HIOs shall perform internal audits to evaluate their process and procedures.

2.1 Evaluation[21]

Under HIPAA security standards, administrative safeguards are required to exchange electronic PHI. Users of HIO exchanges needs to comply with all privacy and security regulations when exchanging electronic health information.

Additionally, periodic technical and nontechnical evaluations are required to reasonably ensure that the covered entity is compliant with the provisions of the HIPAA Security Rule. Audit criteria must be developed and documented in advance for this type of evaluation, known as a "compliance audit." Evaluations shall be performed at least annually and when any major system or business changes occur. The evaluation shall include:

- The generation of a compliance audit findings report,
- Documentation that an identified deficiency has been addressed, will be addressed in order of priority, or represents a risk the organization is willing to accept,
- The documentation on the evaluation shall be retained for minimum of 6 years[22]; however, some states may have longer retention requirements. *POL 17*

[20] IHE: Integrating the Healthcare Enterprise.
[21] HIPAA Security Rule 45 CFR § 164.308 (a)(8) – Evaluation.
[22] 45 C.F.R. § 164.316 (requiring retention for 6 years of policies and any required activity that must be documented under the rule). While 45 C.F.R. § 164.308(a)(8) does not require documentation of the compliance audit, it is a good business practice to do so and to retain that documentation for risk management purposes.

Section 3—Information Access

3.1 Audit Controls[23]

Under HIPAA security standards, technical safeguards are required including policy, data, and system requirements. All entities and their business associates must implement technical processes that accurately record activity related to access, creation, modification, and deletion of electronic PHI. *POL 18*

3.2 Subject of Care Identity

To identify the identity of the subject of care, a matching criteria policy is a required (for example, a match on DOB, First Name, Last Name, Address, etc.). *AUT 2*

AUT 2 Requirements also considered:

The collection and processing of patient demographics includes the collection of SSN and driver's license;
The provider needs to demonstrate proof of the

3.3 Demographics That May Be Logged

An additional audit log should be performed by the HIO for a subset of the subject identity attributes that have been used when a person is found. *DAT 9*

Section 4—Need to Know / Minimum Necessary for Data Management and Release

4.1 Information Disclosure

For purposes of information disclosure, a written policy is required which includes documentation of the following:

- The date and time of the request,
- The reason for the request,
- A description of the information requested, including the data accessed, the data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to another party,
- The ID of person/system requesting disclosure,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information. *AUD 2*

AUD 2 Requirement also considered:

The description of the information requested also includes whether data were printed from another party

[23] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls.

4.2 Auditing Access Where Individual Consent or Authorization is Required

An authorization policy must be in place for any exchange of PHI, and requires the audit log to identify whether the release requires an authorization and, if so, whether the authorization was obtained.

A consent ID would be required, if it exists, for transactions that require a consent or authorization to be tracked for audit purposes. *AUD 2*

Section 5—Need-to-Know Procedure/Process for Personnel Access to PHI

5.1 Information Request

For purposes of information requests, a written policy is required that includes the following components:

- The date and time of the request,
- The reason for the request,
- A description of information requested, including the data accessed, data transmission, any changes to the data (adds, changes, deletes), and whether the data were transmitted to, or printed by another party,
- The ID of person/system requesting disclosure,
- The ID/verification of the party receiving the information,
- The ID of the party disclosing the information,
- The method used for verification of the requesting entity's identity.

An authorization policy must be in place for any exchange of PHI and requires the audit log to identify whether the release requires an authorization and if so, whether the authorization was obtained.

A consent ID is required, if it exists, for transactions that requires a consent or authorization to be tracked for audit purposes. *AUD 1*

5.2 Audit Log Process

The HIO's audit log procedure shall be developed and documented prior to any HIE exchange and shall include identifying who is responsible for reconstitution and sharing audit log information. This includes identifying who is authorized to request the audit log. Also, the procedure shall identify whether the audit log information is available to individuals and how that request is handled. *POL 9*

5.3 Data Authentication

If a document is shared with a patient, methods for assurance shall be established and shall indicate that data have not been modified. *POL 10*

5.4 Preparing a Query Message

When an HIO generates a registry stored query, registry or Record Locator Service (RLS) will be asked if there are records for this patient [Refer to HITSP IS01]. *SYS 1*

SYS 1 Requirement also considered:

The ability of the HIO to generate an HL7 message

Section 6—System Capabilities

6.1 Audit Controls[24]

Audit logs are required to record activity specified by the HIO and the HIO shall periodically review the generated audit logs. This review of the audit logs is based on established audit criteria and shall include documentation of any anomalies. The HIO will document its mitigating action (including sanctions, security incident response team activation, etc. as appropriate). Audit logs must include at least the following: unique user name/ID, date/time stamp, and all actions taken (add, change, delete). Audit logs should either be in readable form or translatable by some easy-to-use tool to be in readable form, and they need to be examined with some frequency appropriate to the HIE to detect improper use. *POL 18*

6.2 Audit Log Content

The HIO's audit logs shall include:

- User ID,
- A date/time stamp,
- Identification of all data transmitted, and
- Any authorizations needed in order to disclose the data. *SYS 3*

The audit log shall include any system activity of use and disclosure of data, and shall retain a record of information systems activity that occurs at established periodic time frames. The audit log for the use and disclosure of data is also required to have a set report in place. Actions that have been identified in the event of discovered anomalies/breaches shall be included in the audit log. Also, login auditing is required as noted under the HIPAA security rule auditing standard. If it exists, any state-specific[25] consent policy under which the data were disclosed shall be tracked. This may be a global consent policy or a specific consent for each access.

If sensitivity restricted information exists, the HIO may choose to implement restrictions as permitted under their state. *SYS 2*

SYS 3 Requirements also considered:

Ability to share responsibilities for identifying what has been transmitted, which entities are responsible for tracking on specifics, and whether data can be transmitted to another party

6.3 Information Integrity

Information integrity is audited by logging that no change has occurred since the signature was applied and shall include a valid date/time stamp. *SYS 12*

[24] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls.
[25] For example, the consent policy of the State of Massachusetts.

6.4 Data Authentication

For purposes of data authentication the use of a valid date/time stamp is required. *AUT 4*

AUT 4 Requirement also considered, but is difficult to implement:

Signature Purpose (ASTM E1762)

6.5 Data Validation

For the purposes of data validation, the signer credentials must be from a trusted authority, and the credential must be current and without constraints, and the credential must be of the appropriate type for the requested data (for example physician or pharmacist). To ensure data integrity, credentials shall indicate that no change has occurred since the signature was applied and must have a valid date/time stamp. *AUT 7*

Requirements Out of Scope

1.0 Electronic Signature SYS 10

SYS 10 Requirement also considered:

Ability for electronic signature (distinct from a digital signature)

2.0 Interim Reports POL 1

POL 1 Requirement also considered:

Interim reports made available for sharing once the ordering physician has signed off on the results, and has been discussed with patient where this is required by policy. There was a difference in state perspective (i.e., border states) about withholding information from a patient

3.0 Returning More Demographics POL 8

POL 8 Requirement Also Considered:

The identification of risk issues– e.g., Data authentication not a high risk in this scenario

4.0 Risk Assessment POL 13

POL 13 Requirement also considered:

The returning of more demographic information to the end user than was entered

5.0 Signature / Data Validation Checking POL 14

POL 14 Requirements also considered:

Signature and Data Integrity conducted prior to allowing the following procedures:
Using data communicated through secured methods (e.g., VPN);
Using data communicated through insecure methods (e.g., patient USB);
Storing data;
Submitting data to shared resource

References

Connecting for Health Common Framework (from the Markle Foundation)—See http://www.connectingforhealth.org/.

M2 – A Model Contract for Health Information Exchange

P2 – Model Privacy Policies and Procedures for Health Information Exchange

P5 – Authentication of System Users

P7 – Auditing Access to and use of a Health Information Exchange

APPENDIX I:
LEGAL REVIEW

See the accompanying document titled **Appendix I HISPC Adoption of Standard Policies Legal Review.doc.**

Coppersmith Gordon Schermer & Brockelman PLC

MEMORANDUM

DATE: April 1, 2009

FROM: Kristen Rosati, Esq.
Coppersmith Gordon Schermer & Brockelman, PLC

RE: Legal Review for the HISPC Phase III Adoption of Standard Policies Collaborative: Identification of Federal and Cross-State Legal Issues in Authentication and Audit Security Policies for Health Information Exchange

The charge of the Adoption of Standard Policies Collaborative (ASPC) is to develop a set of basic policy requirements for authentication and audit for health information exchange (HIE). Through this work, the ASPC hopes to develop processes to help establish trust and bridge the policy differences between different HIE models.

The purpose of this legal report is to discuss federal and potential state legal issues that affect key components of authentication and audit policies in HIE. This work is intended as a general reference source and is not meant to provide legal advice to any person or entity that receives a copy of the work. Readers should consult with competent counsel to determine applicable legal requirements.

I. Introduction

Each state participating in the ASPC worked on key components or elements of their proposed authentication and audit policies that would be applicable to health information organizations (HIOs) or otherwise applicable to the health information exchange (HIE) process in their states. Coming out of that work, the ASPC states worked to develop minimum policy requirements for authentication and audit, to be used across the country to facilitate cross-state HIE.

From the voluminous and carefully considered content in the individual state reports regarding their policies, the Minimum Policy Requirements negotiated by the states, and the final Uniform Security Policy and the Guide to Adoption of Uniform Security Policy, it is obvious that the states participating in the ASPC have put an enormous amount of work into this project. Crafting security policies through a fact-finding and a consensus-based process with stakeholders is hard work, and the ASPC participants should be commended for the work they accomplished.

In this memorandum, I explain various federal statutes and regulations that affect policies for authentication and audit. I also outline a variety of state legal issues that may affect authentication and audit policies to provide guidance to other states that will consider adopting the ASPC's Uniform Security Policy. Because a 50-state law analysis was outside the scope of this project, to demonstrate an analysis of state legal issues, I examined Arizona law applicable

for each issue. Analyses in other states could take a similar approach, but may result in different conclusions. Specifically, this report evaluates the following legal issues:

- HIPAA Privacy and Security, including new developments in the Health Information Technology for Economic and Clinical Health Act (the HITECH Act)
- Notification of breach requirements under the HITECH Act
- Clinical Laboratory Improvement Amendments (CLIA)
- Substance abuse treatment regulations
- FTC Red Flag Rules
- E-SIGN
- Proposed DEA regulations
- State laws that impose authentication and audit requirements in health care, such as
    - statutes or regulations that govern HIOs or the entities participating in HIE;
    - medical record confidentiality statutes or regulations;
    - health care institution licensing statutes or regulations; and
    - pharmacy statutes or regulations that govern e-prescribing
- State laws that impose authentication and audit requirements for all businesses, such as:
    - state security breach reporting requirements;
    - state statutes implementing the Uniform Electronic Transactions Act
- State medical record confidentiality statutes
- State laws regarding social security numbers
- State tort and constitutional laws, including those relating to:
    - tortious invasion of privacy;
    - state constitutional right to privacy;
    - HIPAA as the standard of care in negligence actions;
    - negligence per se claims; and
    - negligence for transmittal of incomplete information.

Because responding to negative audit findings is an important element of a rigorous security policy, Coppersmith Gordon also developed proposed legislation to govern the accountability and enforcement in HIE. This proposed legislation, along with Coppersmith Gordon's research regarding accountability and enforcement mechanisms across the country, is made available through a separate report.

II. The Basics of Authentication and Audit

To assist in review of this report, this section sets forth a basic description of authentication and audit functionality. I also recommend that readers review documents produced by the Connecting for Health Framework on authentication and audit, which are very helpful descriptions of the process and basic requirements.[1]

[1] *See* "Authentication of System Users" at http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf; and "Auditing Access to and Use of a Health Information Exchange," at http://www.connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf.

Authentication is the process of an individual proving he is who he says he is before being allowed access to health information. As described in the Connecting for Health Common Framework report, "[a]uthentication is a way of allowing a user to prove that he is who he claims to be. The simplest form of authentication is in the providing of any identity token plus a secret of some sort, such as a bank card + PIN, or a username + password or phrase."[2] The process of authentication requires the issuance of an identifier:

> An identifier is an attribute that points unambiguously and uniquely to an identity. In practice, the person identifier will often be an employee ID Number, or, possibly, a login name guaranteed unique within the scope of the institution. It is critical that such identifiers not be re-issued to other, later users. If "jsmith" is used as an identifier, all future John or Jane Smiths must be issued a different identifier.[3]

Within the context of the ASPC's work, the term "audit" refers to the process of examining certain defined activity within the health information exchange to monitor whether access to the HIO has been appropriate. (Audit may also refer to the concept of a compliance review of all security policies and their implementation, such as emergency backup plans, training on security, etc., but that is beyond the scope of work for the ASPC.) As noted in the publication, "Information Security Audits":

> Audit logs are one part of [controls that record and examine activity in electronic health information systems] and are used to document access to data, changes or additions to records, sometimes physical access to a secure facility, etc. An important part of any audit is a review of who accessed what when, was access appropriate and if modifications were made. This is needed to make sure access is appropriate, data is protected against inappropriate viewing or modifications, and procedures/process are being followed—all of which are sound business practices.
>
> An audit log is merely an electronic record or a catalog of actions taken. Audit tools to work with audit logs are helpful to sort through what can be an intimidating and, in aggregated [form], useless mound of data. Audit tools assist the auditor and the practitioner in keeping an eye on ongoing activity as well as background for an at least annual full compliance audit.[4]

---

[2] http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf.
[3] *Id.*
[4] Chris Apgar, Information Security Audits, at p. 5 (Nov. 2007) (unpublished manuscript on file with author).

This audit functionality is essential to ensuring accountability in health information exchange, to ensure that the HIO knows what individual accessed what information and when, and then has some process for evaluating whether that access was appropriate under the rules of the HIO.

III. Legal Analysis

A. Federal Law

Current federal law contains very few *specific* requirements related to technical requirements for authentication and audit of access to health information, but instead requires safeguards based on an environment-specific analysis of the risks to health information in the particular system. Federal law *does* contain requirements related to when individual permission is required to access certain information; to the extent the HIO is charged with evaluating whether individual permission has been granted for a particular user to see particular information (i.e. role-based access), that federal law may affect the authentication and audit processes employed by the HIO. Moreover, evolving federal regulations such as the proposed DEA regulations for e-prescribing of controlled substances may in the future contain specific authentication and audit requirements.

In this section, I discuss the requirements of the HIPAA Privacy Standards and the HIPAA Security Standards (as amended by the new HITECH Act), the new HITECH Act notification of breach requirements, the Clinical Laboratory Improvement Amendments (CLIA) and its regulations, the federal substance abuse treatment regulations (the "Part 2" regulations), the Federal Trade Commission's new Red Flag Rules, the federal E-SIGN law, and the proposed DEA regulations governing e-prescribing of controlled substances.

1. HIPAA Privacy Standards

a. Rules Related to Authentication and Audit

The HIPAA Privacy Standards, found at 45 C.F.R. Part 160 and Part 164, Subpart E, contain a basic requirement that a HIPAA covered entity adopt "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information [PHI]."[5] Specifically, covered entities are required to implement safeguards against any intentional or unintentional use or disclosure of PHI in violation of the rules and to "limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure."[6] These requirements apply to covered entities participating in HIE, including hospitals, other institutional providers, most physicians, health care clearinghouses, health plans, and Part D prescription drug plans.[7]

---

[5] 45 C.F.R. § 164.530(c).
[6] *Id.*
[7] 45 C.F.R. § 160.103 (defining HIPAA covered entity); *see also* 42 C.F.R. § 423.505 (h) ("Requirements of other laws and regulations. The Part D plan sponsor agrees to comply with—(2) HIPAA Administrative Simplification rules at 45 CFR parts 160, 162, and 164.").

The HIPAA Privacy Standards also require HIPAA covered entities to include contractually-binding requirements in agreements with individuals and entities acting as "business associates." Simply explained, business associates are third parties that receive PHI in order to perform a function on behalf of a covered entity.[8] Business associate agreements must require business associates to "[u]se appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract."[9] The Health Information Technology for Economic and Clinical Health Act (the HITECH Act), part of the American Recovery and Reinvestment Act of 2009 (the stimulus bill), provides that health information exchange organizations, regional health information organizations, e-prescribing gateways, or vendors that contract with a HIPAA covered entity to allow that covered entity to offer a personal health record to patients as part of its EHR, are business associates if they require access to PHI on a routine basis.[10] Under the HITECH Act, the Department of Health and Human Services (HHS) and State Attorneys General will have the ability to enforce the contractual obligations of business associates, through application of civil and criminal penalties.[11]

The HIPAA Privacy Standards and the Preamble to the regulations (the explanatory information published by the HHS concurrently with the rule), do not contain any description of the particular security practices that would be required for "appropriate administrative, technical, and physical safeguards." So, the HIPAA Privacy Standards do not specifically address authentication or audit requirements, although an effective manner of authenticating individuals before access to electronic PHI (EPHI) and auditing that access surely would be required as part of appropriate safeguards. An HIO should do an assessment regarding whether the ASPC Uniform Security Policy is appropriate for its particular architecture and functionality, to ensure that the HIO is following "appropriate administrative, technical, and physical safeguards."

b. Rules on Access to PHI

The HIPAA Privacy Standards contain extensive rules regarding when a HIPAA covered entity may use or disclose PHI with the individual's permission (called an "authorization" under HIPAA). While a complete discussion of the HIPAA rules on use and disclosure is beyond the scope of this paper, briefly summarized, HIPAA permits the use and disclosure of PHI without authorization for treatment, payment, and "health care operations" (many of the basic business processes of health care entities),[12] as well as many disclosures for public purposes such as public health activities and child abuse reporting.[13]

---

[8] 45 C.F.R. § 160.103 (defining business associate).
[9] 45 C.F.R. § 164.504(e).
[10] Public Law 111-5, Section 13408.
[11] Public Law 111-5, Section 13404 (requiring business associates to comply with 45 C.F.R. § 164.504(e) setting forth the required business associate contract terms, and making HIPAA's criminal and civil penalties applicable to business associates).
[12] 45 C.F.R. § 164.506 (permitting use and disclosure for treatment, payment and health care operations); 45 C.F.R. § 164.501 (definitions).
[13] 45 C.F.R. § 164.512 (listing permitted public purpose disclosures).

If an HIO is permitting access to the PHI in the exchange for purposes other than treatment, payment and health care operations, then individual authorization may be required for access under HIPAA.[14] So, the HIO should evaluate the purposes for which access is allowed, and then determine based on legal advice whether individual authorization is required before access, for purposes of implementing role-based access rules.

c. Rules on Accounting for Disclosures of PHI

The HIPAA Privacy Rule currently requires covered entities to provide an "accounting" of disclosures of an individual's PHI at his or her request, but provides an exception for disclosures made for treatment, payment and health care operations (and a few other reasons). If disclosures are made from an HIO for purposes other than treatment, payment and health care operations, those disclosures should be tracked by the HIO in order to provide the accounting information to individual. An audit trail of information about disclosures from the HIO should capture information that would enable compliance with this HIPAA accounting requirement.

In addition, this accounting obligation will expand in a few years under the new HITECH Act. Section 13405(c) of the HITECH Act provides that disclosures through an electronic health record[15] by a covered entity for treatment, payment and health care operations purposes must be included in the accounting. The Act also requires that disclosures for treatment, payment or health care operations made by business associates "on behalf of the covered entity" must be included in the accounting. HIOs should consult with their counsel about whether the HIO architecture would meet the definition of an "electronic health record" under the HITECH Act, and whether disclosures from the HIO would be "on behalf of" the covered entity. If HIO disclosures should be included, the covered entity may provide the information to the individual; alternatively, the covered entity may provide to individuals a list of the business associates acting on behalf of the covered entity, at which point the business associate would be required to provide the accounting information directly to the requesting individual.

This new accounting requirement applies on January 1, 2014, for entities that acquired an electronic health record before the first of this year, and on January 1, 2011, for entities that acquire an EHR after the first of this year; HHS may delay this by two years through regulation. HHS is required to issue regulations on this issue by June 2010; these regulations presumably will have substantially more detail on what information will need to be included in the accounting. Covered entities and HIOs should examine their audit trails to determine whether they are capturing the information that must be included in the accounting.

---

[14] 45 C.F.R. § 164.512(i) (rules regarding use and disclosure for research).

[15] Section 13400(5) (defining "electronic health record" as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff").

2. The HIPAA Security Standards

The HIPAA Security Standards contain more specific requirements for authentication and audit than do the HIPAA Privacy Standards, but still do not provide detailed guidance for covered entities or their business associates. This lack of specific requirements provides important flexibility in implementing security policies that accommodate different types of environments, but also makes the coordination of policies between covered entities—and between HIOs—challenging because different security risk analyses may lead to different requirements.

Generally, the Security Standards outline four requirements: (1) to ensure the confidentiality, integrity, and availability of all EPHI the entity creates, receives, maintains, or transmits; (2) to protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) to protect against any reasonably anticipated uses or disclosures of the information that are not permitted under the Privacy Standards; and (4) to ensure that the entity's workforce complies with the Security Standards.[16] The regulations specifically provide for flexibility of approach: a covered entity "may use any security measures that allow the covered entity to reasonably and appropriately implement" the regulatory requirements by taking into account: (1) the size, complexity and capabilities of the covered entity; (2) the technical infrastructure, hardware and software security capabilities; (3) the costs of the security measures; and (4) the probability and criticality of potential risks to EPHI.[17]

These general requirements are implemented through required "standards" and "implementation specifications." The standards are divided into the following categories: [18]

- Administrative safeguards: "the administrative functions that should be implemented to meet the security standards [including] assignment or delegation of security responsibility to an individual and security training requirements";[19]
- Physical safeguards: "the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion [including] restricting access to EPHI and retaining off site computer backups";[20] and
- Technical safeguards: "the automated processes used to protect data and control access to data [including] using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as it is being stored and/or transmitted" ;[21]
- Policies and documentation requirements.[22]

---

[16] 45 C.F.R. § 164.306(a).
[17] 45 C.F.R. § 164.306(b).
[18] *See* "Security 101 for Covered Entities" (CMS) at http://www.cms.hhs.gov/EducationMaterials/Downloads/Security101forCoveredEntities.pdf.
[19] 45 C.F.R. § 164.308.
[20] 45 C.F.R. § 164.310.
[21] 45 C.F.R. § 164.312.
[22] 45 C.F.R. § 164.316.

Many of the standards are accompanied by "implementation specifications," which provide more detailed instructions for implementing the standards. As part of the regulators' attempts to allow more flexibility in complying with the Security Standards, these implementation specifications are either "required" or "addressable." The "required" specifications must be implemented as stated in the regulation.[23] However, an entity has more flexibility in dealing with the implementation specifications designated as "addressable"; in that case, the covered entity must perform a security risk assessment of whether the specification is a reasonable and appropriate safeguard in its environment, comparing the specification to its likely contribution to protecting the entity's EPHI. Once the entity has completed an assessment for an addressable specification, an entity may choose, as it deems reasonable and appropriate, to take either of the following actions: (1) implement the specification; or (2) if the specification is not reasonable and appropriate for its environment, document why not and implement a reasonable and appropriate alternative measure that addresses the general standard in a different way.[24]

a. Authentication Requirements

There are a number of standards and implementation specifications that are relevant to the authentication process. First, 45 C.F.R. § 164.308(a)(4)(i), related to information access management, requires policies and procedures for authorizing access to EPHI, so that access to EPHI is consistent with the HIPAA Privacy Standards' substantive requirements on who can see what EPHI for what purpose. The implementation specifications in § 164.308(a)(4)(ii) require:

> (B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
>
> (C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Second, the standard in 45 C.F.R. § 164.312(a)(1), related to implementing access controls, requires a covered entity to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4)." The implementation specification relevant to authentication requires a covered entity to assign a unique name or number for identifying and tracking user identity.[25] This is a required implementation specification. The Centers for Medicare and

[23] 45 C.F.R. § 164.306(d).
[24] *Id.*
[25] 45 C.F.R. § 164.312(a)(2)(i).

Medicaid Services (CMS) publication, "Security Standards: Technical Safeguards"[26] explains that:

> User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. It enables an entity to hold users accountable for functions performed on information systems with EPHI when logged into those systems.
>
> The Rule does not describe or provide a single format for user identification. Covered entities must determine the best user identification strategy based on their workforce and operations. Some organizations may use the employee name or a variation of the name (e.g., jsmith). However, other organizations may choose an alternative such as assignment of a set of random numbers and characters. A randomly assigned user identifier is more difficult for an unauthorized user (e.g., a hacker) to guess, but may also be more difficult for authorized users to remember and management to recognize. The organization must weigh these factors when making its decision. Regardless of the format, unlike email addresses, no one other than the user needs to remember the user identifier.

Third, the standard in 45 C.F.R. § 164.312(d) requires authentication of persons or entities accessing EPHI. It requires "procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." This standard does not contain implementation specifications. In its publication, "Security Standards: Technical Safeguards,"[27] CMS explains:

> In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to EPHI. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:
>
> - Require something known only to that individual, such as a password or PIN.
> - Require something that individuals possess, such as a smart card, a token, or a key.

---

[26] *See* http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf.
[27] *See* http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf.

- Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.

Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system match those stored in that system, the user is authenticated. Once properly authenticated, the user is granted the authorized access privileges to perform functions and access EPHI. Although the password is the most common way to obtain authentication to an information system and the easiest to establish, covered entities may want to explore other authentication methods.

b. Audit Requirements

For audit, the HIPAA Security Standards contain three regulations that require a covered entity to implement an audit program to monitor access to EPHI. First, covered entities are required to have "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."[28] There are no implementation specifications that further detail this standard. The Preamble to the HIPAA Security Standards explains that HHS expects covered entities to have audit controls in place as a technical safeguard, but that covered entities "have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses."[29] The CMS publication, "Security Safeguards: Technical Safeguards"[30] explains:

> It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use EPHI.

Second, the Security Standards require procedures to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[31] Here, too, the specific procedures adopted depend on the covered entity's risk analysis: "The extent, frequency, and nature of the reviews would be determined by the

---

[28] 45 C.F.R. § 164.312(b).
[29] 68 Federal Register (Fed. Reg.) at 8355 (Feb. 20, 2003).
[30] *See* http://www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf.
[31] 45 C.F.R. § 164.308(a)(1)(ii)D).

covered entity's security environment."[32] Third, the Security Standards require procedures for monitoring log-in attempts and reporting discrepancies.[33]

Like the HIPAA Privacy Standards, the Security Standards also require covered entities to contain security requirements in their business associate agreements. The Security Standards permit a covered entity to disclose EPHI to its business associate if it obtains a contract in which the business associate agrees to:

> (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;
> (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
> (C) Report to the covered entity any security incident of which it becomes aware;
> (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.[34]

While the regulations require a business associate to contractually agree to implement administrative, physical and technical safeguards to protect EPHI, the regulations *at this time* do not require a business associate to agree to comply with all of the detailed requirements of the Security Standards.[35] However, under the HITECH Act amendments to the HIPAA Security

---

[32] 68 Fed. Reg. at 8347.
[33] 45 C.F.R. § 164.308(a)(5)(ii)C).
[34] 45 C.F.R. § 164.308(b); § 164.314(a)(2).
[35] In the context of the Privacy Standards, the HHS Office for Civil Rights (which enforces the privacy rule) has explained in its FAQs that business associates are not required to comply with all of the requirements of the HIPAA Privacy Standards:

> Question: Has the Secretary exceeded the HIPAA statutory by requiring "business associates" to comply with the Privacy Rule, even if that requirement is through a contract?
>
> Answer: The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the covered entity comply with its obligations under the Rule.
>
> Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information. (at http://www.hhs.gov/hipaafaq/providers/business/233.html).

Rule, many provisions in the Security Rule will apply directly to business associates on February 17, 2010, a year from the date of enactment.[36]

Moreover, the Security Standards are now being more rigorously enforced by the HHS Office of Inspector General (OIG) on behalf of CMS against covered entities. As noted in "Information Security Audits":

> a recent change in government oversight needs to be taken into account by all organizations, especially HIPAA covered entities. Up until 2007 all HIPAA security enforcement centered on complaints filed with the Center for Medicare and Medicaid Services (CMS). The Office of Inspector General (OIG) on behalf of CMS conducted its first HIPAA security audit at Piedmont Hospital in Georgia. OIG plans to conduct additional random HIPAA security audits during 2008.[37]

Then, on October 27, 2008, the OIG issued a report, "Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight,"[38] which criticized CMS's oversight and enforcement of the HIPAA Security Standards. The OIG stated:

> Ongoing Office of Inspector General audits of various hospitals nationwide indicate that CMS needs to become more proactive in overseeing and enforcing implementation of the HIPAA Security Rule by focusing on compliance reviews. Preliminary results of these audits show numerous, significant vulnerabilities in the systems and controls intended to protect ePHI at covered entities. These vulnerabilities place the confidentiality and integrity of ePHI at high risk. During our audit, CMS began taking steps to conduct compliance reviews. After we completed our fieldwork

---

> While this commentary relates to the Privacy Standards, CMS likely would take the same position on the HIPAA Security Standards, because the Security Standards similarly do not contain language that requires business associates to comply with all of the specific terms and conditions of those regulations. This will change on February 17, 2010, when the HITECH Act becomes law and applies the Security Standards to HIPAA business associates.

[36] Public Law 111-5, Section 13401(a) ("Application of Security Provisions—Sections 164.308 [administrative safeguards], 164.310 [physical safeguards], 164.312 [technical safeguards], and 164.316 [policies and documentation] of title 34, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security [notification in the case of breach] and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.").

[37] Apgar, *Information Security Audits* (Nov. 2007).

[38] *See* http://oig.hhs.gov/oas/reports/region4/40705064.pdf.

> but before we issued our report, CMS executed a contract to conduct compliance reviews at covered entities.

The HITECH Act will require HHS to conduct periodic audits of both covered entities and their business associates.[39] It also increases the civil penalties,[40] and provides enforcement authority to State Attorneys General to enforce the HIPAA Privacy and Security Rules, including seeking injunctions, damages on behalf of individuals, and attorneys' fees.[41] These new penalties and State AG enforcement authority are effective immediately.

In its Uniform Security Policy, the ASPC has proposed minimum standards for HIOs to include in their authentication and audit policies. These minimum policy components meet the terms of the HIPAA Security Standards, as long as when they are implemented by an HIO, the HIO conducts a security risk assessment of its particular environment and concludes that these minimum policy components adequately protect EPHI in the HIO's system. The specifics of an HIO's authentication and audit practice should be established after a risk assessment of its environment, based on an analysis of (1) the size, complexity and capabilities of the HIO; (2) the technical infrastructure, hardware and software security capabilities; (3) the costs of the security measures; and (4) the probability and criticality of potential risks to EPHI.

3. Notification in the Case of Breach: HITECH Act

Section 13402 of the HITECH Act creates a new federal notification of breach requirement for HIPAA covered entities and their business associates. HHS must issue interim final regulations to implement this section within 180 days, or by August 16, 2009. Covered entities and business associates then will be required to comply with the Act's breach reporting requirements for breaches discovered starting 30 days after HHS issues regulations.

This section requires a covered entity that "accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach." A covered entity's business associate is required to notify the covered entity of such breach by the business associate.

This new reporting requirement hinges on two important definitions:

- **Unsecured protected health information:** Section 13402(h) defines this term as PHI that is not secured through the use of a technology or methodology specified by HHS guidance. HHS is required to issue annual guidance, starting May 16, 2009, regarding the technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute." If HHS does not issue guidance, then covered entities

[39] Public Law 111-5, Section 13411 (audits).
[40] Public Law 111-5, Section 13410 (new tiered civil penalties).
[41] Public Law 111-5, Section 13410(e) (State AG enforcement authority).

and business associates must comply with standards issued by an ANSI-accredited organization. If a covered entity or business associate complies with HHS guidance (or other standards in the absence of HHS guidance), then its information would be "secured" and a breach would not be reportable. On the other hand, if a covered entity or business associate does not comply with HHS guidance (or other standards in the absence of HHS guidance), it will have "unsecured PHI."

- **Breach**: Section 13400 defines "breach" as follows:

> (A) In general.--The term "breach" means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
>
> (B) Exceptions.--The term ``breach" does not include--
> (i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if--
> (I) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and
> (II) such information is not further acquired, accessed, used, or disclosed by any person;
>
> or
>
> (ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility;
>
> and
>
> (iii) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

This means that unintentional or inadvertent access to information in an entity's EHR HIO by employees of the covered entity is not a reportable breach unless that employee further uses or discloses the PHI in an unauthorized manner. On the other hand, intentional

unauthorized access to information in an EHR by an employee is a breach and is reportable if that information is not "secured" under the HHS guidance.[42]

It will not be clear until HHS issues its regulations how this will apply to access to information held by HIOs. The statute makes an exception for unintentional access "by an employee or individual acting under the authority of a covered entity or business associate" if the access was in good faith and "within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate." I would argue that, as long as the individual inadvertently accessing the information in an HIO is an employee of or otherwise acts under the authority of a covered entity participant in the HIO, the terms of the statutory exception are met. This would make sense, as well, because the purpose of the exception appears to be avoiding the burden of reporting where access to an individual's information is a mistake by someone who is otherwise authorized to see health information and no further use or disclosure is made of the information.

New breach reporting requirements apply to other non-HIPAA covered entities that are not business associates, as well. Section 13407 of the Act requires personal health record (PHR) vendors, entities that provide products or services through the Web site of PHR vendors, and non-covered entities that access or send information to a PHR, to notify each citizen or resident of the United States of a breach of security where "unsecured PHR identifiable information" was acquired by an unauthorized person as a result of the breach; these entities also are required to notify the Federal Trade Commission. These entities' "third party service

---

[42] The Act contains rigorous notification requirements:

- *Individuals notified; timing*: Covered entities must notify "each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach" without unreasonable delay and in no case later than 60 days of discovery of the breach by the covered entity or its business associate (unless there is a law enforcement request for delay).
- *Manner and form of notice*: Notice must be made by first-class mail (or email if specified by an individual). If there is insufficient or out-of-date contact information, a covered entity must do a "substitute form of notice"; if there are more than 10 individuals affected, the entity must do a conspicuous Web site posting or notice in major print or broadcast media.
- *Notice to the media:* If more than 500 residents of the State are involved, the entity must provide notice to "prominent media outlets."
- *Self-disclosure to HHS*: If more than 500 residents of the State are involved, the entity must provide immediate notice to HHS. If fewer than 500 residents are involved, the entity must log the breach and disclose it to HHS in an annual report.
- *Content of notice*: The regulations require the notice to individuals to contain a description of what happened and the unsecured PHI involved, steps for individuals to protect themselves, a description of the covered entity efforts to investigate, mitigate and prevent further breaches, and contact information.

A business associate is not required to provide notice of breach to the individual. Rather, a business associate must notify the covered entity of a breach, along with identification of each affected individual.

providers" are required to provide notice to the entities, rather than to the FTC. The failure to comply will be an "unfair and deceptive act or practice" under the FTC Act. Like HHS, the FTC is required to issue regulations within six months, and the reporting requirements will be applicable 30 days later.

Many questions remain that hopefully will be answered by the FTC regulations when issued. The PHR vendor breach notification has slightly different standards than the breach notification requirement for covered entities and their business associates. For example, the PHR vendor breach reporting applies upon any acquisition of an individual's information without authorization of the individual, but does not contain the exceptions to reporting for unintentional access where there is no further use or disclosure. Also, it is unclear whether this reporting requirement will apply to business associates such as HIOs that supply PHI to a PHR on behalf of an individual; the statute section purports to apply to "entities that are not covered entities and that access information in a personal health record or send information to a personal health record," which would include HIOs.

Moreover, breach reporting is made more complicated, because state breach reporting statutes continue to apply if the state reporting requirements are more stringent than the federal provisions. Section 13421 of the Act applies the HIPAA state law preemption standards at 42 U.S.C. § 1320d-7. This supersedes any "contrary" provision of State law, except when the state law is "more stringent" than HIPAA. State laws are generally "more stringent" if they provide greater rights to individuals or greater privacy protection.

To avoid triggering the federal and any state breach reporting requirements, an HIO should have rigorous authentication and audit policies. HIOs will need to pay close attention to the HHS regulations (and for PHR vendors, the FTC regulations), and the HHS guidance on how to secure PHI, as the details in those regulations and guidance documents may impact the information that needs to be captured through the audit trail, the timing of the audits (to be able to capture breaches quickly), and other information for compliance purposes.

4. CLIA

The federal Clinical Laboratory Improvement Amendments (CLIA) and its regulations govern the operations of certified clinical laboratories. The statute and its regulations do not contain rules on authentication and audit. However, rules regarding to whom clinical laboratory results may be released may impact an HIO's implementation of role-based authentication for access.

CLIA regulations permit laboratories to release test results "only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test."[43] An "authorized person" is defined by the CLIA regulations as "an individual authorized under State law to order tests or receive test results, or both."[44] CLIA thus defers to state law regarding who is authorized to receive clinical laboratory test results.

[43] 42 C.F.R. § 493.1291(f).
[44] 42 C.F.R. § 493.2.

This deferral to state law poses a particular challenge in states without law on this issue. In Arizona, for example, the law is silent regarding whether a clinical laboratory may provide lab results to an HIO and whether an HIO may release the results to non-ordering physicians for treatment purposes. Interestingly, the Arizona clinical laboratory statutes exempt all CLIA-certified laboratories from state regulation, so the Arizona clinical laboratory statutes do not apply to CLIA-certified labs, which include all clinical laboratories in Arizona producing lab results for patient treatment.[45] Arizona law is thus silent on who is an "authorized person" to receive lab results for purposes of CLIA. The Arizona Department of Health Services (ADHS) provided a "substantive policy statement"[46] that permits clinical laboratories in Arizona to release lab results to an HIO, at least in the context of a federated HIE model where the HIO does not itself store the laboratory results.[47] Because CLIA defers to state law to define who is

---

[45] A.R.S. § 36-461 (exempting all CLIA-certified laboratories from Title 36, Chapter 4.1, Article 2).

[46] A substantive policy is advisory only and does not impose additional requirements or penalties on regulated parties or rules made in accordance with the Arizona Administrative Procedure Act. It is a helpful document to clarify ADHS interpretation of existing law.

[47] ADHS Substantive Policy Statement # SP-001-OD-OACR ("CLINICAL LABORATORY RELEASE OF PATIENT TEST RESULTS TO A HEALTH INFORMATION EXCHANGE ORGANIZATION"):

> A.R.S. § 36-470 is … instructive for CLIA certified laboratories. CLIA regulations require an "authorized person" to order laboratory tests and direct test results to be released only to "authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." 42 C.F.R. §493.1241 and 493.1291. An "authorized person" is "an individual authorized under State law to order tests or receive test results or both." 42 C.F.R. §493.2. Therefore, CLIA regulation points to state law to determine what parties may receive clinical laboratory test results.
>
> A.R.S. § 36-470(A) permits any person licensed under Title 32, Chapters 7 (Podiatry), 8 (Chiropractic), 11, Article 2 (Dentistry), 13 (Medicine and Surgery), 14 (Naturopathic physicians), 17 (Osteopathic physicians), and 29 (Homeopathic physicians) to order tests to be completed at a clinical laboratory. Additionally, persons licensed to practice medicine or surgery in another state or a person authorized by law or department rules may order tests to be completed at a clinical laboratory. A.R.S. § 36-470(A). A.R.S. § 36-470(B) directs a clinical laboratory to report test results to the person who authorized the laboratory test. Arizona law is silent on any other disclosure of clinical laboratory test results.
>
> However, federal law provides further direction as to clinical laboratory test disclosures. HIPAA permits clinical laboratories to report test results to a non-ordering physician in order to treat a patient. 45 C.F.R. §164.506. Both clinical laboratories and physicians are HIPAA covered entities permitted to share patient information for the purposes of treatment. Also, HIPAA permits disclosure of a patient's protected health information to an [HIO] if the [HIO] has the required business associate agreement.
>
> As defined above, the [HIO] would not receive or store clinical laboratory results. The role of the [HIO] is to facilitate communication between the patient's health care provider and entities, such as clinical laboratories, that possess clinical laboratory test results. According to the Department's interpretation, A.R.S. § 36-470 neither permits nor prohibits a clinical lab from disclosing clinical laboratory test results to an [HIO].

an "authorized person" that may receive lab results, each state should carefully examine its own clinical laboratory laws.

Where state law is silent on who is an "authorized person" to receive lab results, there is one other potential avenue for releasing lab results to treating, non-ordering physicians through HIE. In addition to an individual authorized under state law to receive lab results, CLIA regulations also permit release of lab results to an "individual responsible for using the test results,"[48] but do not define what that means. One interpretation is that a non-ordering physician who has a treatment relationship with a patient falls within this definition because the treating physician would utilize the test results in treating the patient. This interpretation would also be consistent with 42 C.F.R. § 493.1291(g), which requires a laboratory to "immediately alert the individual or entity requesting the test and, if applicable, the individual responsible for using the test results when any test result indicates an imminently life-threatening condition, or panic or alert values"; this phrase indicates an intention that results be released to treating physicians, even if they did not request or order the test. CLIA program personnel at CMS have not yet issued guidance on whether a treating, non-ordering physician is an "individual responsible for using the test results," and if so, whether this would also support release to an HIO on behalf of those physicians.

5. Federal Substance Abuse Treatment Regulations

The federal regulations governing alcohol and drug abuse treatment information, called the "Part 2 regulations" because they are found at 42 Code of Federal Regulations Part 2,[49] apply to any "federally assisted" alcohol or drug abuse "program."[50] While the Part 2

> Because there is no prohibition on such a disclosure in Arizona law, disclosure of a patient's clinical laboratory test results to an [HIO] consistent with HIPAA does not conflict with state law. Therefore, the Department believes a clinical laboratory may share clinical laboratory test results with an [HIO] when done in compliance with HIPAA.

[48] 42 C.F.R. § 493.1291(f).
[49] See 42 C.F.R. §§ 2.1 through 2.67.
[50] 42 C.F.R. § 2.3. A "program" is a person or entity that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment, or referral for treatment. 42 C.F.R. § 2.11. A program is "federally assisted" if it: (1) is conducted entirely or in part by any federal agency or department (with some exceptions for Veterans Administration and Armed Forces programs); (2) is conducted under a license, certificate, registration, or other authorization from any federal agency or department, including certified Medicare providers, authorized methadone maintenance treatment providers, and programs registered under the Controlled Substances Act to dispense controlled substances for alcohol or drug abuse treatment; (3) is tax-exempt or to whom contributions are tax deductible; or (4) is the recipient of any federal funds. 42 C.F.R. § 2.12(b). The types of programs that may be covered include treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, school-based programs, and private practitioners who hold themselves out as providing, and do provide, alcohol or drug abuse diagnosis, treatment, or referral for treatment, if they are federally assisted. A general medical facility is not a "program" unless it has a discrete, identified unit that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment, or referral for treatment, so these federal regulations do not have wide applicability.

regulations do not have requirements related to authentication and audit, the Part 2 regulations may affect whether substance abuse treatment information may flow into an HIO and rules for role-based authentication to obtain that information from the HIO.

Some health systems, hospitals or other providers participating in HIE may operate federally-assisted substance abuse treatment "programs" and will need to carefully consider what information they provide to an HIO. Any "disclosure" of substance abuse treatment information by a federally-assisted substance abuse treatment program must comply with the regulations; a disclosure to an HIO *may* be permitted as a disclosure to a "qualified service organization" (an organization that provides services to the program), if the program has a written agreement in place with the HIO in which the HIO agrees to be fully bound by the Part 2 regulations.[51]

In addition, even if an entity participating in HIE is not directly covered by the Part 2 regulations because it does not operate a federally-assisted substance abuse treatment program, that entity may be required to comply with these regulations with regard to information it *receives* from a federally-assisted substance abuse treatment program. First, third party payers that receive records[52] disclosed by federally-assisted substance abuse treatment programs are required to comply with the Part 2 regulations.[53] Third party payers are broadly defined as including a person or entity "who pays, or agrees to pay, for diagnosis or treatment furnished to a patient on the basis of a contractual relationship with the patient or a member of his family or on the basis of the patient's eligibility for Federal, State, or local governmental benefits."[54] This will apply to both public and private health plans.

Second, any person or entity who receives records directly from a federally-assisted substance abuse treatment program and who is notified by the program that the records are protected by the Part 2 regulations, must also comply with these regulations with regard to that information.[55] If a program requires a patient's consent to release the patient's records (as a program is required to do for most purposes, other than release of records for emergency treatment), the program must include a written statement that warns the recipient that the recipient may not further disclose the information unless permitted by the Part 2 regulations.[56] So, an entity that receives confidential substance abuse information from a substance abuse program, and receives this written notice with the information, must follow the Part 2

---

[51] 42 C.F.R. § 2.11 (defining qualified service organization); § 2.12(c)(4) (permitting disclosure to a qualified service organization).
[52] "Records" include "any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program." 42 C.F.R. § 2.11 (definitions).
[53] 42 C.F.R. § 2.12(d)(2)(i).
[54] 42 C.F.R. § 2.11 (definitions).
[55] 42 C.F.R. § 2.12(d)(2)(iii).
[56] 42 C.F.R. § 2.32 (requiring written statement: "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.").

regulations in redisclosing that information. That might occur if the program receives consent to release the information to another treating provider in a non-emergency situation, or to a health plan to get paid. (The federal government has not yet provided guidance on how this written notice requirement would be handled in the context of electronic HIE.)

Many providers that maintain substance abuse treatment programs segregate this sensitive information from the rest of the information on the provider's electronic health information system, and thus have protections in place that prevent the inclusion of protected information in disclosures to external parties. However, many plans and providers that *receive* this information from substance abuse programs do not have adequate mechanisms for segregating this information electronically.

The Part 2 regulations set forth substantial restrictions on the use and disclosure of protected information. Essentially, patient consent is required except for disclosures for emergency treatment and a few other permitted disclosures.[57] However, the HHS Substance Abuse and Mental Health Services Administration (SAMHSA), Center for Substance Abuse Treatment, has clarified that the Part 2 regulations only protect information that can identify a patient as an alcohol or drug abuser or someone who has applied for or received that type of treatment: "This allows a program that is part of a larger entity, such as a hospital, to disclose information about a patient so long as it does not explicitly or implicitly disclose the fact that the patient is an alcohol or drug abuser."[58] This means that substance abuse treatment programs that are part of larger entities, and the health plans and providers (and HIOs) that receive protected information from the substance abuse treatment programs, would be permitted to use and disclose patient information in HIE as long as that information does not indicate that the patient was a substance abuser or had applied for or received such treatment. If the information indicates that the patient was a substance abuser or applied for or received this treatment, patient consent would be required or disclosure must be limited to treatment for emergencies only.

---

[57] *See* 42 C.F.R. § 2.12, § 2.13, § 2.51, § 2.52, and § 2.53. These permitted disclosures include:
(1) To communicate internally in connection with duties related to the provision of diagnosis, treatment or referral for treatment of alcohol or drug abuse;
(2) To communicate with an entity that has direct administrative control over the program;
(3) To notify law enforcement officers when a patient commits or threatens to commit a crime on the premises or against program personnel;
(4) To report suspected child abuse and neglect as required by state law;
(5) To medical personnel for the purpose of treating a condition that poses an immediate threat to the health of any individual and that requires immediate medical intervention;
(6) To the Food and Drug Administration ("FDA") for purposes of notifying patients and their physicians of dangers to the health of any individual due to mislabeling, error in manufacture, or the sale of products under FDA jurisdiction;
(7) For research activities, but only if certain protections are followed;
(8) To communicate with "qualified service organizations" (third party business partners that provide data processing, legal services, and other functions for the program); and
(9) Audit and evaluation activities of the program.

[58] SAMHSA, The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs" (June 2004), at http://www.hipaa.samhsa.gov/download2/SAMHSAHIPAAComparisonClearedPDFVersion.pdf.

6. FTC Red Flag Rules

Last year, the Federal Trade Commission (FTC) issued regulations to prevent identity theft (called the "Red Flag Rules"), which *may* affect the authentication and audit policies of an HIO, depending on the functions of the HIO.[59] The FTC Red Flag Rules require that "creditors" that offer or maintain one or more "covered accounts" develop and implement a written identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with the covered accounts.[60] These regulations originally were effective on November 1, 2008, but the FTC has delayed enforcement until May 1, 2009.[61]

A "creditor" is any person (or entity) that regularly extends, renews, or continues credit[62]; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.[63] It came as a great shock to the health care industry that many health care providers are covered by these rules; a provider that allows patients to pay for medical services *after* the services are provided or through installment payments is considered by the FTC to be a "creditor" under these regulations. If an HIO offers any types of services on credit to consumers or to participating health care providers, it will be considered a "creditor" required to have an identity theft prevention program in place (if it maintains covered accounts). The evolving business models of HIOs across the country must be evaluated to consider whether the HIO would be a creditor under the FTC rules. For example, HIOs that offer health banking or personal health record services to consumers may function as creditors if they provide services before receiving payment. Similarly, HIOs that offer services to health care providers, such as hosted EMRs, transaction-based information exchange, or other services, may also function as creditors if they provide those services before receiving payment.

If an HIO is acting as a creditor, then the next step would be to determine whether it has "covered accounts," which include: (1) an account with consumers "primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions"; or (2) any account, including those established for business purposes, "for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the … creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[64] So, an HIO would maintain a "covered account" and be subject to these regulations if it: (1) had accounts with consumers; or (2) its accounts with business customers had a reasonably foreseeable risk of identity theft. Where an HIO stores electronic health information or patient demographic information in an "account" for a participating provider,

---

[59] *See* 72 Fed. Reg. 63718 (Nov. 9, 2007).
[60] *See* 16 C.F.R. § 681.2(d)(1).
[61] *See* http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf.
[62] "Credit" means "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor." 16 C.F.R. § 681.2(b)(4); 15 U.S.C.A. § 1681a(r)(5); 15 U.S.C.A. § 1691a(d). It is not limited to credit granted to individual consumers.
[63] 16 C.F.R. § 681.2(b)(5); 15 U.S.C. § 1681a(r)(5); 15 U.S.C.A. § 1691a(e).
[64] 16 C.F.R. § 681.2(b)(3).

the FTC could conclude that this poses a foreseeable risk of identity theft that would require an identity theft prevention program to be in place.

So, if an HIO is a creditor that maintains covered accounts under the FTC Red Flag Rules, the HIO must implement an identity theft prevention program that is appropriate to its size and complexity and the nature and scope of its activities. The required program must include reasonable policies and procedures for detecting and responding to a "red flag"—a pattern, practice, or specific activity that may indicate identity theft—in connection with its covered accounts.[65] An HIO would also be required to do a number of administrative actions.[66]

The Red Flag Rules do not specify what a red flag may be in the context of health information exchange. HIOs should consider what suspicious activities might indicate identity theft. For example, if it permits consumers to access information in the HIO directly (as in a health banking model), multiple log-in attempts to a personal account or the addition of demographic or medical information into an account that is inconsistent with the existing record may indicate access for the purpose of identity theft. In the context of health care provider access to information in the HIO, multiple log-in attempts may indicate an unauthorized person attempting to gain access; this may be a red flag because unauthorized access to health information databases often may be to secure information to use in identity theft. Another red flag might be the provision of suspicious documents (such as forgeries of a medical license) to gain a username and password to the system; the FTC has indicated that the greatest risk of identity theft was in the opening of a new account.[67] Again, the HIO should consider this issue in the context of its particular architecture, function and the information available in the HIO.

The Red Flag Rules also do not specify what the policies and procedures for detecting and responding to these red flags must include, but it is likely that a rigorous authentication and audit process should be part of those procedures.

In summary, as noted above, some HIOs *may* be creditors that maintain covered accounts under the FTC Red Flag Rules. In that case, they would be required to have procedures in place to identify and respond to potential identity theft. The ASPC has recommended authentication processes that rely on trusted third parties to authenticate individuals before providing access to the HIO. HIOs should look at their specific processes to

---

[65] 16 C.F.R. § 681.2(b)(9); 16 C.F.R. § 681.2(d)(2).

[66] 16 C.F.R. § 681.2(e):

- Obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors;
- Involve the board of directors, an appropriate board committee, or a designated senior management level employee in the program's oversight, development, implementation;
- Train staff to effectively implement the program;
- Exercise appropriate and effective oversight of service provider arrangements;
- Provide for the continued administration of the program; and
- Ensure the program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

[67] 72 Fed. Reg. 63718, 64727.

ensure there is a process in place for those third parties to evaluate whether documents submitted are authentic in support of an application for a username and password.

The ASPC also has recommended audit processes, but many have not specified what those practices should be. While those details may be developed later, HIOs that are subject to the FTC Red Flag Rules should have details in their audit practices that indicate unauthorized access to health information to identify potential identity theft.

7. E-SIGN

The Electronic Signatures in Global and National Commerce Act (E-SIGN), codified at 15 U.S.C., Chapter 96, is intended to facilitate the use of electronic records and electronic signatures in interstate commerce. It states that a contract or signature "may not be denied legal effect, validity, or enforceability solely because it is in electronic form." The E-SIGN law does not place any negative restrictions on the use of electronic signatures to sign medical records or other documents transmitted to or through an HIO, does not set forth any specific requirements for electronic signatures, and does not contain any specific authentication or audit requirements.

8. Proposed DEA Regulations

Some HIOs are considering hosting electronic prescribing (e-prescribing) functionality. If they do so, the authentication methods adopted for access to the system for e-prescribing (or at least for e-prescribing of controlled substances) will be affected by Drug Enforcement Agency (DEA) regulations.

In June of 2008, the DEA issued proposed regulations to govern the e-prescribing of controlled substances.[68] DEA regulations currently prohibit the use of e-prescribing for controlled substances; the proposed regulations propose to allow e-prescribing by physicians and to permit pharmacies to receive, dispense, and archive electronic prescriptions under strict conditions. As described by the DEA:

> DEA implements the Comprehensive Drug Abuse Prevention and Control Act of 1970, often referred to as the Controlled Substances Act (CSA) and the Controlled Substances Import and Export Act (21 U.S.C. 801-971), as amended. DEA publishes the implementing regulations for these statutes in Title 21 of the Code of Federal Regulations (CFR), Parts 1300 to 1399. These regulations are designed to ensure an adequate supply of controlled substances for legitimate medical, scientific, research, and industrial purposes, and to deter the diversion of controlled substances to illegal purposes. The CSA mandates that DEA establish a closed system of control for manufacturing, distributing, and dispensing controlled substances. Any person

[68] 73 Fed. Reg. at 36721 (June 27, 2008).

> who manufactures, distributes, dispenses, imports, exports, or conducts research or chemical analysis with controlled substances must register with DEA (unless exempt) and comply with the applicable requirements for the activity.
> ***
> The CSA and DEA's regulations were originally adopted at a time when most transactions and particularly prescriptions were done on paper. The CSA mandates that some records must be created and kept on forms that DEA provides and that many controlled substance prescriptions must be manually signed.[69]

There are a number of provisions in the DEA's proposed regulations (which are not yet final and may change), which would affect authentication and audit in e-prescribing mechanisms involved in HIE:

- The DEA will require in-person identity proofing. The DEA proposes to allow only DEA-registered hospitals, state professional licensing boards, or state or local law enforcement agencies to review the required identity documents and to sign a certification that the individual prescriber is who the applicant claims to be. This identity document must be a government-issued id with photo.

- The DEA will require two-factor authentication, where one factor is stored on a hard token that can be maintained by the prescriber. This hard token could include a PDA, a cell phone, a smart card, a thumb drive, or a multi-factor one time password token. This factor cannot be stored on a computer that is not a portable hardware device that the prescriber can keep in her possession. The prescriber must notify the service provider within 12 hours of discovery of the loss or compromise of the token, or the prescriber will be held responsible for any prescriptions written using the token.

- The DEA proposes to require a variety of security requirements for systems and service providers that market software and services for e-prescribing to prescribers and pharmacies. These rigorous requirements are set forth in full in Appendix A, in the event that HIOs are planning to function as the system or a service provider for e-prescribing.

The DEA's proposed authentication requirements for e-prescribing of controlled substances are substantially more stringent than what the ASPC recommends in the Uniform Security Policy. Specifically, the in-person identity proofing by a limited number of entities, two-factor authentication with one factor stored on a hard token maintained by the prescriber, and many of the security requirements for systems and service providers that market software and services for e-prescribing to prescribers and pharmacies, are not consistent with the proposed minimum rules on authentication and audit proposed by the ASPC. If these DEA regulations are finalized in their present form, HIOs may wish to consider having a separate

[69] 73 Fed. Reg. at 36722.

authentication process for e-prescribing or for e-prescribing of controlled substances; to use the same authentication process for all access to the HIO may impose operationally difficult and expensive authentication requirements for access to the HIO.

B. State Law

A variety of state legal issues will potentially affect the policies on authentication and audit, particularly if an HIO is implementing role-based authentication to govern who can access what type of information. While providing guidance on role-based access was not within the scope of the ASPC, this memorandum identifies potential legal issues related to authentication and audit, including role-based access, to support additional work in this area in the future. Once again, a 50-state analysis is outside the scope of the legal work for the ASPC, but to demonstrate the type of analysis that would be required in each state, I examine Arizona law applicable to issues that may affect authentication and audit policies.

1. State Laws That Impose Authentication and Audit Requirements in Health Care

Some states may have statutes or regulations that impose specific authentication or audit requirements applicable to the health care industry. For example, legal representatives should consider whether their states have the following types of laws and whether those laws contain authentication or audit requirements:

- statutes or regulations that govern HIOs or the entities participating in health information exchange (HIE);
- medical record confidentiality statutes or regulations;
- health care institution licensing statutes or regulations; or
- pharmacy statutes or regulations that govern e-prescribing.

Example analysis of state law: In Arizona, for example, we do not presently have laws that apply to HIOs or entities participating in HIE. Moreover, Arizona's medical records laws do not contain any specific requirements related to authentication or audit. Arizona has a general health information confidentiality law[70] and special restrictions on the disclosure of mental health information by licensed behavioral health providers,[71] genetic testing information,[72] HIV/AIDS and other communicable disease information,[73] but these laws do not contain requirements for authentication and audit. Similarly, Arizona health care institution licensure regulations[74] do not contain specific security requirements. Arizona's pharmacy statutes,[75]

---

[70] Arizona Revised Statutes (A.R.S.) § 12-2291 through § 12-2296.
[71] A.R.S. § 36-501 *et seq*.
[72] A.R.S. §§ 12-2802**{** TA \l "A.R.S. §§12-2802" \s "A.R.S. § 12-2802" \c 2 **}**.
[73] A.R.S. § 36-664**{** TA \s "A.R.S. § 36-664" **}**.
[74] *See* R9-10-209 (patient rights requirements for hospitals); R9-10-228 (medical records requirements for hospitals); R9-10-505 (patient rights requirements for adult day health care facilities); R9-10-511 (medical records requirements for adult day health care facilities); R9-10-710 (patient rights requirements for assisted living facilities); R9-10-714 (medical records requirements for assisted living facilities); R9-10-802 (general requirements for hospices, including patient rights); R9-10-812 (medical records requirements for

pharmacy regulations,[76] and the Arizona Uniform Controlled Substances Act[77] do not contain specific authentication or audit requirements. While the Arizona Uniform Controlled Substances Act would appear to prohibit e-prescribing of controlled substances, the Board of Pharmacy regulations permit e-prescribing of controlled substances if the prescriber and pharmacy follows applicable federal law.[78]

2. State Laws That Impose Authentication and Audit Requirements for All Businesses

Legal representatives should also look for state statutes or regulations that govern good security practices for all business in the state. For example, if the state has a breach reporting law, it may affect how the HIO should structure its authentication or audit program (such as the requirement to perform monitoring to detect security breaches, which might require certain methods or timing of the audits). Each state should examine whether its breach reporting law is preempted by the new federal breach reporting requirements under the HITECH Act. (See Section III(A)(3).)

HIOs should also examine if their states have statutes or regulations governing electronic signatures that might be used during the HIE process, which laws may have specific requirements for authentication in the e-signature process. Most states have implemented the Uniform Electronic Transactions Act (or "UETA"). The UETA is a Uniform Act proposed by the

---

hospices); R9-10-907 (patient rights requirements for nursing care institutions); R9-10-913 (medical records requirements for nursing care institutions); R9-10-1107 (patient rights requirements for home health agencies); R9-10-1108 (medical records requirements for home health agencies); R9-10-1403 (patient rights requirements for recovery care centers); R9-10-1409 (medical records requirements for recovery care centers); R9-10-1507 (patient rights requirements for abortion clinics); R9-1511 (medical records requirements for abortion clinics); R9-10-1703 (patient rights requirements for outpatient surgical centers); R9-10-1710 (medical records requirements for outpatient surgical centers); A.R.S. § 32-1401 (allopathic physicians) (defining "unprofessional conduct" as including "[i]ntentionally disclosing a professional secret or intentionally disclosing a privileged communication except as either act may otherwise be required by law," interpreted as permitting physicians to comply with HIPAA); A.R.S. § 32-101 (naturopathic physicians) (same); A.R.S. § 32-1854 (osteopathic physicians) (same); A.R.S. § 32-2933 (homeopathic physicians) (same).

[75] Title 32, Arizona Revised Statutes, Chapter 18.

[76] Arizona Administrative Code, Title 4, Chapter 23 (Board of Pharmacy rules).

[77] A.R.S. § 36-2501, *et seq.; see* A.R.S. § 36-2525 (requiring manually signed written prescription for controlled substances).

[78] R4-23-407. Prescription Requirements

***

"F. Electronic transmission of a prescription order from a medical practitioner to a pharmacy.

1. Unless otherwise prohibited by law, a medical practitioner or medical practitioner's agent may transmit a prescription order by electronic means, directly or through an intermediary, including an E-prescribing network, to the dispensing pharmacy as specified in A.R.S. § 32-1968.

2. For electronic transmission of a Schedule II, III, IV, or V controlled substance prescription order, the medical practitioner and pharmacy shall ensure that the transmission complies with any security or other requirements of federal law.

3. The medical practitioner and pharmacy shall ensure that all electronic transmissions comply with all the security requirements of state or federal law related to the privacy of protected health information."

National Conference of Commissioners on Uniform State Laws (NCCUSL). The purpose of the UETA is to harmonize state laws to recognize the validity of electronic signatures and electronic storage of documents. A list of states that have accepted UETA can be found on the NCCUSL Web site.[79] The Web site indicates that Georgia, Illinois, New York, and Washington have not adopted UETA, but these states are reported as having other laws recognizing electronic signatures.[80] Because the UETA is not *itself* an enforceable law, each state should look to its own law that adopts the UETA (or an alternative electronic signatures law) to determine any specific requirements for authentication in the use of electronic signatures.

Example analysis of state law: Arizona's security breach reporting law does not contain specific requirements regarding authentication and audit, although it does require notification of consumers if the entity becomes aware of a security breach of unencrypted personal information through its audit program.[81] (An analysis of the HITECH Act notification of breach requirement is in Section III(A)(3) above.)

Arizona has adopted the UETA through the Arizona Electronic Transactions Act (AETA),[82] which gives electronic signatures the same validity and enforceability as written signatures. AETA's definition of an "electronic signature" is "an electronic sound, symbol or process, attached to or logically associated with a record and that is executed or adopted by an individual with the intent to sign the record."[83] Under this law, an electronic signature "satisfies any law that requires a signature."[84] An electronic signature is attributable to a person if the signature was the act of the person or the person's electronic agent,[85] which may be shown in any manner, including the adoption of a "security procedure" that verifies that an electronic signature is of a specific person, such as algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgement procedures.[86] A signature is a "secure electronic signature" if:

> through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:
> 1. Unique to the person using it.
> 2. Capable of verification.
> 3. Under the sole control of the person using it.
> 4. Linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

---

[79] *See* http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp.
[80] http://en.wikipedia.org/wiki/Uniform_Electronic_Transactions_Act.
[81] A.R.S. § 44-7501.
[82] A.R.S. § 44-7001, *et seq.*
[83] A.R.S. § 44-7002(8).
[84] A.R.S. § 44-7007(D).
[85] A.R.S. § 44-7009(A).
[86] A.R.S. § 44-7002(14). See also Section 44-7031 (defining "secure electronic signature" to create a rebuttable presumption that the record was not altered).

Arizona also has a more prescriptive law governing electronic signatures on documents filed with or by state agencies.[87] These security procedures required for e-signatures clearly require an authentication process to ensure that the individual sending the signed document is the person claimed.

3. State Medical Record Confidentiality Statutes

Many states have statutes or regulations that provide a greater level of protection for information related to HIV and other communicable diseases, mental health, substance abuse, genetic testing, and sometimes other types of information. These state laws may affect an HIO's implementation of role-based authentication for access to health information because these laws will specify who can see what information.

In determining how state health information confidentiality laws affect release of information by HIOs, and thus the role-based access rules that need to be in place, states should examine three questions. First, the state should determine whether its various state health information confidentiality laws apply to disclosures by an HIO. State health information confidentiality laws usually have varying applicability to different entities in the health care system. Some state statutes and regulations apply only to certain types of providers; for example, a state's mental health laws may apply to disclosures by licensed behavioral health providers, but may not apply to hospitals. Other state laws may have broader application to any entity or person who handles or receives sensitive information, such as information that an individual has received genetic testing. The first element of analysis for the application of state health information confidentiality laws, then, is to determine the laws' scope of application—do they apply to disclosures by an HIO?

The second element of analysis for the application of state health information laws is to determine whether those laws apply to the particular type of information that will be flowing through the HIO. For example, it is possible that genetic testing information will be segregated by the data sources and will not be transmitted through the HIO. On the other hand, many medical records contain information regarding communicable diseases, so it is likely that communicable disease information will flow to the HIO.

Finally, in evaluating the impact of state health information confidentiality laws, the analysis should consider whether existing consent processes cover the proposed use of the information. For example, if a community seeks patient consent to disclose health information to the HIO, the consent form should be examined to determine whether it will cover sensitive information, such as HIV test information, if that information will be available from the data sources to the HIO.

Example analysis of state law: With that framework in mind, the following discussion explores the application of the Arizona genetic testing law on the release of health information

[87] *See* 41-132 (requiring "[a]n electronic signature shall be unique to the person using it, shall be capable of reliable verification and shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated"; containing specific requirements for an electronic signature that is a digital signature through the use of an asymmetric cryptosystem).

to an HIO in Arizona. Similar genetic testing laws are very common throughout the United States and likely will affect the disclosure of genetic testing information to an HIO. Before enactment of the Genetic Information Nondiscrimination Act (GINA), which protects individuals against discrimination in health insurance and employment,[88] many states enacted rigorous state laws controlling genetic testing and the disclosure of the resulting information to protect individuals against insurance and employment discrimination.[89] These state laws are not preempted by GINA and will continue to govern the disclosure of genetic testing information to an HIO, and the HIO's subsequent disclosures to others.

In Arizona, for example, the results of a genetic test are confidential and may be released only for the purposes expressly listed in the statute (including for treatment of a patient).[90] Moreover, when a person (or entity) has received genetic testing information from someone else, the recipient also must follow the state statutory rules on disclosing that information.[91] Information and records held by a state agency or a local health authority relating to genetic testing information are confidential and are exempt from public copying and inspection.[92] Finally, health plans are subject to even more restrictive rules on disclosing genetic testing information, and may not release those results to any party without the written, express consent of the subject of the test.[93] Applying our decision elements discussed in the introduction to this section, the analysis would be as follows:

(1) Does the law apply to disclosures of genetic testing information to an HIO (or subsequent disclosures of genetic testing received by the HIO)? Yes. In Arizona, the genetic testing statute applies to any recipient of genetic testing information.

(2) Does the law apply to the particular type of information received? Arizona's genetic testing statute applies to "a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies."[94] An HIO would need to evaluate whether this type of information will be provided to the HIO.

(3) Do existing consent processes cover release of the information? In Arizona, a consent for release of genetic testing information must be specific to genetic testing.[95] General consents gathered by a health system or health plan therefore would not suffice for release of genetic testing information to an HIO, or the HIO's subsequent release of that information, unless it specifically included genetic testing.

---

[88] *See* National Human Genome Research Institute Web site, at http://www.genome.gov/24519851.
[89] *See, e.g.*, Genetic Alliance Web Site at http://www.geneticalliance.org/ws_display.asp?filter=about; Electronic Privacy Information Center Web Site at http://www.epic.org/privacy/genetic/.
[90] A.R.S. §§ 12-2802.
[91] A.R.S. § 12-2802(F).
[92] A.R.S. § 12-2804.
[93] A.R.S. § 20-448.02.
[94] A.R.S. §§ 12-2802(1).
[95] A.R.S. § 12-2802(A)(3) (permitting release to "[a]ny person who is specifically authorized in writing by the person tested or by that person's health care decision maker to receive this information.").

4. State Laws Regarding Social Security Numbers

Under HIPAA, a driver license number and SSN are HIPAA "identifiers" and thus must be treated as PHI subject to both the HIPAA Privacy and Security Rules.[96] Many states are adopting laws that more strictly regulate the use and disclosure of SSN. State legal representatives should examine these laws to determine whether the inclusion of SSN in information provided to the HIO would impose role-based access requirements for that information.

Example analysis of state law: In Arizona, for example, A.R.S. 44-1373 places restrictions on the disclosure of SSNs by all persons or entities in the state. Unless specifically permitted by another law, the Arizona statute provides that a person or entity in Arizona shall not:

> 1. Intentionally communicate or otherwise make an individual's social security number available to the general public.
>
> 2. Print an individual's social security number on any card required for the individual to receive products or services provided by the person or entity.
>
> 3. Require the transmission of an individual's social security number over the Internet unless the connection is secure or the social security number is encrypted.
>
> 4. Require the use of an individual's social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the site.
>
> 5. Print a number that the person or entity knows to be an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This paragraph does not prohibit the mailing of documents that include social security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number. In a transaction involving or otherwise relating to an individual, if a person or entity receives a number from a third party, the person or entity has no duty to inquire or otherwise determine if the number is or includes that individual's social security number. The person or entity may print that number on materials that are mailed to the individual, unless the person or entity that received the number has actual knowledge that the

[96] 45 C.F.R. § 164.514.

> number is or includes the individual's social security number. This paragraph does not prohibit the mailing to the individual of any copy or reproduction of a document that includes a social security number if the social security number was included on the original document before January 1, 2005.[97]

The statute does not define "general public." It *may* prohibit inclusion of an SSN on a document available to HIE participants, although it is unlikely the Arizona Attorney General would interpret HIE participants as the general public, because HIE participants will be subject to confidentiality and other restrictions in the HIE participation agreement. Moreover, the law does not prohibit "the collection, use or release of a social security number as required by the laws of this state or the United States or for internal verification or administrative purposes."[98] So, I don't believe this Arizona statute would prohibit the release of an SSN to an HIO for patient demographic matching purposes, or to HIE participants if the SSN is included in documents exchanged through HIE, as long as the Internet transmission is secure or the SSN is encrypted. However, given the concern with identity fraud and medical identity theft, an HIO might consider implementing a method for redacting SSNs from documents provided to third parties through HIE.

5. State Tort and Constitutional Laws

Finally, legal representatives should examine whether their states have case law that requires a certain standard for authentication or audit in order to meet the standard of care for negligence actions or to meet state constitutional requirements. For example, legal representatives should examine their case law on tortious invasion of privacy and other common law actions that may affect the authentication and audit practices implemented by HIOs in that state. In the following sections, I discuss Arizona law that might be applicable; this is a guide to the type of analysis that would need to be done in each state. Each state may have substantially different common law, however, and this analysis should be specific to the HIO's state.

From a liability perspective under state law, I anticipate that most states will not have case law that specifies what level of authentication and audit are required; rather, most tort case law requires an entity to act reasonably in light of all the circumstances. It will thus assist in avoiding liability if HIO policies meet good business practices applied throughout the health care industry, including the model security policies developed through the HISPC project and other industry guidance, such as National Institute of Standards and Technology (NIST).[99]

Whatever authentication or audit policy is chosen by an HIO, it is very important that the HIO follow its policy. As Chris Apgar notes in his publication, *Information Security Audits* at p. 6 (Nov. 2007):

---

[97] A.R.S. 44-1373(A).
[98] A.R.S. 44-1373(C).
[99] *See, e.g.,* National Institute of Standards and Technology (NIST), "Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 REV 1), at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

> The bottom line is if you do not intend to review audit logs generated, say, from a particular application, it is often better not to turn on the audit logs If audit logs are generated, they need to be reviewed at least randomly. The generation of audit logs that are not monitored creates a significant potential liability for the organization. These audit logs are discoverable in the event of litigation and, if not looked at and a problem is found, the organization is at higher risk of liability than if the audit logs had not been generated in the first place.

I agree with this analysis. The authentication and audit choices must reasonably protect the health information in possession of the HIO (or handled by the entities participating in HIE), but choices that are too ambitious will not be achievable and may cause additional liability.

In addition to having rigorous authentication and audit policies—and following those policies—HIOs should consider other methods of reducing liability as a result of inappropriate use by others of the information in the HIO. For example, the HIO should have participation agreements in place that place terms and conditions on access to information in the exchange and subsequent duties of confidentiality.[100] The HIO should also consider messages or disclaimers to append to every access, such as: "This message, including any attachments, is intended solely for the use of the named recipient and may contain confidential and privileged information. Unauthorized access will subject the user to potential criminal and civil penalties." This will remind authorized users about their confidentiality duties and also alert non-authorized recipients that they are about to access confidential information.

[100] For a sample HIO participation agreement developed in Arizona on behalf of Arizona Health-e Connection, see http://www.azhec.org/BinaryData/PDFs/HII/AzHeC%20Model%20HIE%20Participation%20Agreement%20(4-17-08).pdf.

a. Tortious Invasion of Privacy

Most states recognize a tort action for invasion of the right of privacy, which is the "right to be let alone."[101] According to the Restatement (Second) of Torts, the right of privacy can be invaded in one of four generally recognized ways:

- unreasonable intrusion upon the seclusion of another;
- appropriation of the other's name or likeness;
- unreasonable publicity given to the other's private life;
- publicity that unreasonably places the other in a false light before the public.[102]

Most cases involving a breach of the security or privacy of health information would involve allegations of invasion of privacy based upon an alleged unreasonable intrusion upon plaintiff's seclusion. The Restatement describes the tort of intrusion upon seclusion as "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, … if the intrusion would be highly offensive to a reasonable person."[103] According to the Restatement (Second) of Torts, a plaintiff must demonstrate by a preponderance of the evidence each of the following elements to prevail on an invasion of privacy claim based on intrusion upon seclusion:

- an objectively reasonable expectation of seclusion or solitude in a place, conversation or data source; and
- an intentional, highly offensive, intrusive act into such place, conversation or data source.[104]

A plaintiff's expectation of privacy in her medical records generally would be objectively reasonable, depending on the terms under which the health information is provided to the HIO. The HIPAA Privacy Standards and most state health information confidentiality laws provide that health information is confidential and may disclosed only in certain circumstances.[105]

However, it is unlikely that a plaintiff could demonstrate that an HIO committed an "intentional, highly offensive, intrusive act" unless an HIO (or an agent of the HIO)

---

[101] Restatement (Second) of Torts, § 652A, Comment a (1977) (defining the right to privacy). *See, e.g., Reed v. Real Detective Publishing Co.*, 63 Ariz. 294, 162 P.2d 133 (1945) (first Arizona case recognizing an action for invasion of privacy).
[102] Restatement (Second) of Torts, § 652A(2)(a)-(d).
[103] *Hart*, 947 P.2d at 853 (quoting Rest. § 652B).
[104] Restatement (Second) of Torts, § 652A (1977). *See Godbehere*, 62 Ariz. at 339-40, 783 P.2d at 785-86; *Medical Laboratory Management Consultants*, 30 F. Supp. 2d at 1187-1190.
[105] *See, e.g.* A.R.S. § 12-2292 (unless otherwise provided by law, "all medical records and payment records, and the information contained in medical records and payment records, are privileged and confidential. A health care provider may only disclose that part or all of a patient's medical records and payment records as authorized by state or federal law or written authorization signed by the patient or the patient's health care decision maker.").

intentionally discloses a patient's health information, or unless the HIO has completely inadequate security procedures in place that would reflect reckless disregard for protecting the patient's health information. (For example, if the HIO had an authentication process in place that fell well below the standard of care in the industry, it is possible that a court could conclude that the HIO's actions are intentional.) Of course, each state should look to its case law on what type of conduct constitutes an "intentional, highly offensive, intrusive act." In Arizona, for example, there is no state law on the issue, but the federal Ninth Circuit Court of Appeals advises that offensiveness is determined by considering "the degree of the intrusion, the context, conduct and circumstance surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[106] So, the motives of the HIO likely will be relevant to determining whether a cause of action for invasion of privacy may stand.

b. Constitutional Right to Privacy

Legal representatives should also examine whether their state constitution includes a right of privacy and how that would affect disclosures by the HIO policies on authentication and audit. For example, Article 2, Section 8 of the Arizona Constitution establishes a constitutional right of privacy: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." Arizona's constitutional right to privacy does not, however, provide a cause of action for invasion of privacy between private individuals or entities.[107]

c. HIPAA as the Standard of Care in Negligence Actions

Courts consistently have concluded that HIPAA does not create a private right of action for violation of the requirements of HIPAA.[108] However, some cases have applied the HIPAA regulations to establish the underlying standard of care in a claim for breach of privacy or negligence.[109] So, the HIPAA Security Standards authentication and audit requirements could be relevant to a tort action brought under state common law.

---

[106] *Medical Laboratory Management Consultants,* 30 F. Supp. 2d at 1189 (*quoting Deteresa v. American Broadcasting Companies, Inc.*, 121 F.3d 460, 465 (9th Cir. 1997)).
[107] *See Cluff,* 10 Ariz. App. 560, 563, 460 P.2d 666, 669, overruled on other grounds by *Godbehere v. Phoenix Newspapers, Inc.*, 162 Ariz. 335, 783 P.2d 781 (1989) ("This constitutional provision was not intended to give rise to a private cause of action between private individuals, but was intended as a prohibition on the State and has the same effect as the Fourth Amendment of the Constitution of the United States.").
[108] *See, e.g., Webb v. Smart Document Solutions, LLC,* 499 F.3d 1078, 1082 (9th Cir.2007); *Buchanan v. Gay,* 491 F. Supp. 2d 483 (D. Del. 2007); *Acara v. Banks,* 470 F.3d 569 (5th Cir.2006); *Agee v. United States,* 72 Fed.Cl. 284 (Fed.Cl.2006); *Carney v. Snyder,* No. C.A. 06-23 ERIE, 2006 WL 2372007 (W.D.Pa. Aug.15, 2006); *Rigaud v. Garofalo,* No. Civ.A. 04-1866, 2005 WL 1030196 (E.D.Pa. May 2, 2005); *O'Donnell v. Blue Cross Blue Shield of Wyoming,* 173 F.Supp.2d 1176, 1179-80 (D.C.Wyo.2001); *Wright v. Combined Insur. Co. of Am.,* 959 F.Supp. 356, 362-63 (N.D.Miss.1997).
[109] *See, e.g. Sorensen v. Barbuto,* 143 P.3d 295 (Utah App. 2006) (involving patient claim against former treating physician after physician engaged in ex parte communications with defense counsel in patient's underlying personal injury action).

While the HITECH Act does not create a new private right of action under HIPAA, it does provide enforcement authority to State Attorneys General to enforce the HIPAA Privacy and Security Rules, including seeking damages on behalf of individuals.[110]

d. Negligence Per Se

Ordinarily, the scope of the tort duty of care is established by common law. Under the doctrine of negligence per se, however, the standard of conduct to which a defendant will be held may be defined as that required by statute, rather than as the usual "reasonable person" standard under common law. According to the Restatement (Second) of Torts, a court may adopt statutory requirements as the standard of conduct for a negligence action if the statute is intended:

- to protect a class of persons which includes the one whose interest is invaded;
- to protect the particular interest which is invaded;
- to protect that interest against the kind of harm which has resulted, and
- to protect that interest against the particular hazard from which the harm results.[111]

Each state should evaluate whether its medical records confidentiality laws or other state laws noted in the sections above could give rise to a negligence per se claim in their state.

e. Negligence for Transmittal of Incomplete Information

The ASPC also inquired about potential liability for failure to transmit complete information. Due to state health information confidentiality laws and an HIO's role-based authentication, some information may be withheld or redacted by the HIO (or by the data source) to comply with those laws. The HIO's agreement with participants should set forth the parameters of the data provided and should alert the participants about the conditions under which the data may not be complete due to confidentiality restrictions (if applicable to the particular state).

A notice attached to the particular message where information has been withheld or redacted is also desirable to reduce liability, but is substantially more difficult to implement. This is an area of substantial national dialog. The National Committee on Vital and Health Statistics (NCVHS), a federal advisory body that advises HHS on health data, statistics and national health information policy, issued a report on February 20, 2008, in which the NCVHS recommended that the Secretary of HHS implement a policy for the National Health Information Network (NHIN) to allow individuals to "have limited control, in a uniform manner, over the disclosure of certain sensitive health information for purposes of treatment."[112] NCVHS expressed concern about "protecting patients' legitimate concerns about privacy and confidentiality, fostering trust and encouraging participation in the NHIN in order to promote opportunities to improve patient care, and protecting the integrity of the health care

---

[110] Public Law 111-5, Section 13410(e) (State AG enforcement authority).
[111] *Good v. City of Glendale*, 150 Ariz. 218, 221, 722 P.2d 386, 389 (App. 1986) (citing the Restatement (Second) of Torts, § 286 (1965)).
[112] http://www.ncvhs.hhs.gov/080220lt.pdf.

system." NCVHS thus recommended an open public process to uniformly decide across the country which categories of health information an individual would be permitted to sequester from access through the NHIN without express consent (such as information related to domestic violence, genetic information, mental health information, reproductive health, and substance abuse). At the same time, the NCVHS recognized "that the technologies and human factors needed to implement the recommendations in this letter are not necessary readily available for the EHR systems, HIEs, and other components of the emerging NHIN." This is a situation where HIE architecture and available technology may have to catch up with desired policy outcomes.

NCVHS also recognized that, if certain information is sequestered from access, there should be some form of notification to providers accessing the incomplete information. Because that discussion is directly on point, I excerpt the entire section of the NCVHS report on notification of information sequestration here:

> **Notations of missing data for Health Care Providers**
> When patients are provided an opportunity to choose categories of information for sequestration, NCVHS believes that it is important that a notation is made to the provider that some information in the record is not being made available at the request of the patient. We understand that it is possible that a notation in the record might reveal more information than would be available under current practice. For example, the HHS regulations regarding substance abuse treatment do not give a provider information about the sequestration of a record of substance abuse treatment. In the fragmented health records system we have today, moreover, patients can withhold information from their providers and be reasonably confident that the information will not be disclosed. Nevertheless, NCVHS concluded that, where permitted by law or regulation, health care providers should be notified when information is being sequestered in order to increase providers' trust in the contents of the record. If a provider knew that patients could sequester information but they would not be notified, providers could never really trust that their records were accurate and complete, and would be hesitant to treat patients based on those records. The inclusion of some notation that information is missing alerts a provider that caution and special care are appropriate. Furthermore, a significant advantage of the notation is that it provides an opportunity for providers to discuss with their patients concerns about the sequestration of information and the resulting impact on their health care.
>
> There are at least two approaches to how the notation should be accomplished. One solution would be to give a general notice that information has been sequestered without any indication of what

> categories were designated by the patient. This approach potentially increases privacy for the patient because the nature of a category, such as mental health information, might, by itself, reveal the sequestered information. For routine care, a care provider might not need to see the sequestered information and most of the time it would remain hidden. A disadvantage of this approach is that it may require health care providers to question patients about every category routinely in an attempt to determine whether any relevant information is missing, increasing the burden on providers and ultimately resulting in a system less protective of privacy and less efficient.
>
> Another approach is that the sequestered category should be noted, permitting the provider to make a more informed judgment as to whether the category is likely to be relevant to the current encounter, and only to ask the patient when it seems appropriate. This approach has the potential to be more efficient, and, since most of the time sequestered information would remain hidden, it could adequately protect the patient's privacy. A disadvantage of this approach is that some categories, by themselves, reveal sequestered information, such as that a patient has a mental health or substance abuse record, and designations of specific categories of sequestered information would not be adequately protective of patient privacy.
>
> NCVHS acknowledges that it does not yet know exactly how such a notation process would work. The success of the process will likely depend on the enumerated categories, the breadth of their definitions, and the frequency with which patients sequester information. These are the types of issues that should be explored in future hearings and investigated through pilot projects and research.
>
> ***
>
> Recommendation 1c. The design of the NHIN should ensure that when a health care provider accesses health information with one or more categories sequestered, a notation indicates that sensitive health information has been sequestered at the direction of the patient. The specificity of the notation will need to be determined.

In summary, HIOs should carefully watch the development of this issue, and should at the very least notify providers accessing information in the HIO that some information may be withheld or redacted by the HIO (or by the data source) to comply with federal and state confidentiality laws.

IV. Conclusion

The Adoption of Standard Policies Collaborative has developed a set of basic policy requirements for authentication and audit for HIE, as documented in its Uniform Security Policy. This model policy will help establish trust and bridge the policy differences between different HIO models, to assist in cross-HIO and interstate HIE. As this memorandum explores, there are many federal and state laws that may affect an HIO's authentication and audit policies. This memorandum hopefully will assist HIOs across the country in evaluating these laws to determine whether they may adopt the Uniform Security Policy and what potential modifications they may need to make to conform to various legal requirements.

Kristen Rosati

Appendix A: Summary of DEA Proposed Regulations for E-Prescribing Systems and Service Providers, quoted from 73 Fed. Reg. at 36739-40 (June 27, 2008)

► The electronic prescription service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing of prescribing practitioners regarding the conduct of the in-person identity proofing. The document may be prepared on the identity proofing entity's letterhead or other official form of correspondence, or the service provider may design a form for use by the identity proofing entity. Regardless of the format, the document must contain certain information required by DEA. Entities DEA is proposing to permit to conduct in-person identity proofing of prescribing practitioners include:

- the entity within a DEA-registered hospital that has previously granted the practitioner privileges at the hospital (e.g., a hospital credentialing office);
- the State professional or licensing board, or State controlled substances authority, that has authorized the practitioner to prescribe controlled substances;
- a State or local law enforcement agency;
- the service provider must check both the practitioner's State license and DEA registration to determine that both are current and in good standing.

► Authentication: Access to the electronic prescribing system for the purposes of signing prescriptions must meet the standards for Level 4 authentication in NIST SP 800-63. That is, the system must require at least two-factor authentication to access the system; one factor must be a cryptographic key stored on a hard token that meets the requirements for Level 4 authentication in NIST SP 800-63 or a multi-factor one time password token. The hard token must be a hardware device that meets the following criteria:

- The token must require entry of a password or biometric to activate the authentication key.
- The token is not able to export the authentication key.
- The token must be validated under Federal Information Processing Standard (FIPS) 140-2 as follows:
    - overall validation at Level 2 or higher.
    - physical security at Level 3 or higher.

► The security of the system must be audited annually using a third-party audit that meets the requirements of a SysTrust or WebTrust audit for security and processing integrity.

► The system must limit signing authority to those practitioners that have a legal right to sign prescriptions for controlled substances (i.e., the system must set varying levels of access to the system based on responsibilities).

► The system must have an automatic lock out if the system is unused for more than 2 minutes.

► The prescription must contain all of the required data (date of issuance of the prescription; patient name and address; registrant full name, address, DEA registration number; drug name, dosage form, quantity prescribed, and directions for use; and any other information

specific to certain controlled substances prescriptions mandated by law or DEA regulations). Prior to signing the controlled substance prescription, the system must show the prescribing practitioner at least the patient name and address, drug name, dosage unit and strength, quantity, directions for use, and the DEA number of the prescriber whose identity is being used to sign the prescription.

► Where more than one prescription has been prepared for signing, prior to authenticating to the system the practitioner must positively indicate which prescription(s) are to be signed.

► The practitioner must authenticate himself to the system immediately before signing a prescription.

► After authenticating to the system but prior to transmitting the prescription, the system must present the practitioner with a statement indicating that the practitioner understands that he is signing the prescription being transmitted. If the practitioner does not so indicate, by performing the signature function, the prescription cannot be transmitted.

► The system must transmit the electronic prescription immediately upon signature. The system must not transmit a controlled substance prescription unless it is signed by a practitioner authorized to sign such prescriptions.

► The electronic data file must include an indication that the prescription was signed.

► The system must not allow printing of prescriptions that have been transmitted; if a prescription is printed, it must not be transmitted.

► The system must generate a monthly log of controlled substance prescriptions and transmit it to the practitioner for his review. The practitioner must indicate that the log was reviewed. A record of that indication must be maintained for five years.

► The first recipient of the prescription must digitally sign the prescription and archive the digitally signed version of the prescription as received.

► The first pharmacy system that receives the prescription must digitally sign and archive a copy of the prescription as received. Alternatively, the intermediary that transmits the prescription to the pharmacy may digitally sign the transmitted prescription and transmit both the record and the digitally signed copy for the pharmacy to archive.

► The digital signatures must meet the requirements of FIPS 180-2 and 186-2.

► The pharmacy system must check to determine whether the DEA registration of the prescribing practitioner is valid. (Alternatively, any of the intermediary systems may conduct this check provided that the record indicates that the check has been conducted. The CSA database may be cached for one week from the date of issuance by DEA of the most current database.)

► The pharmacy system must be able to store the complete DEA number including extensions.

► The pharmacy system must have an audit trail that identifies each person who annotates or alters the record. The pharmacy system must conduct daily internal audits to identify any auditable events.

► The system must have a backup system of records stored at a separate location.

► The pharmacy system must have a third-party audit that meets the requirements of SysTrust or SAS 70 audits for security and processing integrity.

► The contents of a controlled substance prescription must not be altered, other than by reformatting, during transmission.

► A prescription created electronically for a controlled substance must remain in its electronic form throughout the transmission process to the pharmacy; electronic prescriptions may not be converted to other transmission methods, e.g., facsimile, at any time during transmission.

APPENDIX J:
STAKEHOLDER COMMENTS AND RECOMMENDATIONS

Stakeholder Feedback on Uniform Security Policy

The ASPC sent a draft of the Uniform Security Policy for review by Stakeholders in 11 states on February 6, 2009. We received considerable interest in the policy and in many cases the comments were positive with no suggested changes other than grammatical. The Policy was distributed through 11 different states and Stakeholders were requested to vet the policy against existing or planned security policies, to see how best they could work with an exchange with another HIO, both intra- and interstate. Feedback was incorporated into the final draft of the guide, upon final review by the ASPC legal workgroup. Following are some of the comments received.

Table J-1. Stakeholder Feedback on Uniform Security Policy: Recommendations

Recommendation	Action
Our policy writers discovered that the first requirement for authentication was the enactment of a use agreement between parties/HIOs and this language needed to be in the policy. Although Markle Foundation Model Contract language was used, one of the Stakeholders reviewing the policy was on the DURSA contracting workgroup of the NHIN and offered an alternative section for the policy.	Replaced the Use Agreement requirement section in the Policy.
It was noted that the feasibility of every entity complying with security rules depends on the complexity, technical ability of each entity, and cost to that entity of adhering to the rules (implementation and maintenance). Several Stakeholders requested additional clarity of terminology used in the policy, especially technical terms referred to as a requirement.	Following review, the glossary was amended to reflect new or expanded terms.
Several commenters requested additional language or terminology to be added to the Uniform Security Policy to reflect their business model, technical and/or operational environment in their state. Others requested additions to reflect the privacy and security laws in their state. There was confusion in the understanding that the policy was a negotiated consensus of minimum security policy requirements for authentication and audit, and should establish a floor to the security requirements for each HIO.	The Policy is an appendix in the Guide for Adoption best explains its use.

Table J-2. Stakeholder Feedback on Uniform Security Policy: Positive Feedback

Positive Feedback
"Thanks again for giving us the opportunity to review your work. I'm sure you are proud of the work you and your team(s) have done in this area."
"This is an extremely well-written document … I applaud you all for the obvious attention to detail and the significant amount of effort that must have gone into its completion."
"Thank you for letting me review the draft policy and thanks to all for the hard work that went into getting the draft published."
One ASPC state reported that none of the stakeholders that I have communicated with has anything but complimentary things to say about the Security Policy.
"Our Critical Access Hospital, HIE was very complimentary on the ease of use and commented that they believe this tool will be valuable for them going forward. In discussion with the 'statewide' HIE, they were concerned that some of the policies did not apply as clearly to them, as they would with their end users' EHRs."
"The representatives from our community reviewed the potential impact of the proposed basic security policy and requirements. We are in agreement that the security policies must be widely adopted across the community to be successful. Overall, the document flowed well and we commend the structure of the writing. "

Stakeholder Feedback on Adoption Guide

The ASPC sent a draft of the Adoption Guide for review by Stakeholders on March 17.

We received both constructive feedback, which helped in shaping the final draft of the guide, and positive feedback about the envisioned usefulness of the guide. Following are some of the comments received:

Table J-3. Stakeholder Feedback on Adoption Guide: Recommendations

Recommendation	Action
Because this seems like it would be overwhelming, especially to beginners just trying to jump into the HIE world and are especially concerned about privacy and security, suggest a summary of the whole document (a "quick guide to the Guide") placed near the beginning, for beginners who might get lost in the details unfamiliar to them. This should bring a higher success rate to getting people to read and use the Guide.	Added an overview section at the beginning of the guide
… there needs to be a consistent framework and wording that conveys the central point that the Guide may be used from various perspectives, the following two probably being the primary ones: (a) those entities that are adopting new policies; (b) those that need to verify that their current policies, procedures, and practices meet the minimum requirements and possibly make some minor changes of what they already have in place.	Added into narrative as needed

Table J-4. Stakeholder Feedback on Adoption Guide: Positive Feedback

Positive Feedback
"Excellent guide, very understandable and user friendly."
Praise for Checklist as being an especially useful feature.
"This report represents a lot of work. It is really well organized and Appendix B is very well laid out and clear. The checklist seems like a well-thought out, methodical approach to something very complex. "
"I reviewed this Guide with the thought of comparing the policies your group is recommending with our existing policies (that are quite extensive and have stood well the test of time). I wanted to know what changes, if any, would be needed in our policies (procedures and practices) and 'if,' and/or, 'how' the changes would (or might) influence our current risks and situation. I appreciated the part about methods to get to appropriate and already-vetted standards. That part was especially helpful."

APPENDIX K:
CONTRIBUTORS

Arizona

Kim Snyder
Project Director
Government Information Technology Agency, State of Arizona
Principal, Illumine IT Solutions

Emilie Sundie, MSCIS
Project Manager
Government Information Technology Agency, State of Arizona
Principal, The Sundie Group

Kristen B. Rosati, JD
Coppersmith Gordon Schermer & Brockelman PLC

Colorado

Arthur Davidson, MD, MSPH
Director, Public Health Informatics and Preparedness
Denver Public Health Department
Associate Professor, Department of Family Medicine, School of Medicine
Department of Community Medicine, Colorado School of Public Health
University of Colorado at Denver

Connecticut

John T. Lynch, MPH
Executive Director
Connecticut Center for Primary Care

Lori Reed-Fourquet, MSCS
Consultant, e-HealthSign LLC
Vice Convenor, TC215 Health informatics WG4 Security and Privacy
Co-Chair, ASTM E31.25 Healthcare Data Management, Security, Confidentiality, and Privacy

Michael J. Purcaro, MS, PT
Executive Director
The Public Health Foundation of Connecticut, Inc.

Maryland

David Sharp, MLA, PhD
Director, Center for Health Information Technology
Maryland Health Care Commission

Nebraska

David P. Lawton, RN, PhD
Public Health Informatics Manager
Nebraska Department of Health and Human Services

Ann Fetrick, RN, PhD
University of Nebraska Medical Center
College of Public Health, Center for Biosecurity, Biopreparedness & Emerging Infectious Diseases

Anne Byers, EdM
Community Information Technology Manager
Nebraska Information Technology Commission

Ohio

Mary M. Crimmins, MA, CPEHR, CPHIT
Research Associate, Center for Healthy Communities
HISPC Liaison, HealthLink RHIO
Wright State University
Boonshoft School of Medicine

Philip Powers
Director of Technology
Health Policy Institute of Ohio

Oklahoma

Lynn Puckett
Contract Services Director
Oklahoma Health Care Authority

Ann F. Chou, PhD, MPH
Assistant Professor
College of Public Health & College of Medicine
University of Oklahoma

Utah

Francesca Lanier, MA
Project Director
Office of Public Health Informatics
Utah Department of Health

Virginia

Chris Doucette
Privacy Officer
Virginia Department of Medical Assistance

Kim Barnes
Policy Analyst/Medical Information
Virginia Department of Health

Reneé Kelley
Compliance & Security Analyst
Virginia Department of Medical Assistance

Washington

Jeffrey Hummel, MD, MPH
Medical Director for Clinical Informatics
Qualis Health
Associate Clinical Professor
Internal Medicine, University of Washington
Founder and Chief Medical Officer
Deep Domain, Inc.

Jordana Huchital, MS
Principal and Consultant
Interactive Outcomes

Technical Advisory Panel

Gary G. Christoph, PhD, CIPP, CHS, CISM
HHS Client Executive
Northrop Grumman Corporation

Chris Apgar, CISSP
President
Apgar & Associates, LLC

RTI International

David Harris, MPH
RTI International