March 31, 2009

Health Information Security and Privacy Collaboration

Guide to Adoption of Uniform Security Policy

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

Guide to Adoption of Uniform Security Policy

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

Figures

Tables

1. INTRODUCTION

This Guide to Adoption of Uniform Security Policy ("Adoption Guide") was developed by the Adoption of Standard Policies Collaborative (ASPC), part of the Health Information Security and Privacy Collaboration (HISPC) initiative. Sponsored by the Office of the National Coordinator for Health Information Technology, HISPC was formed to address privacy and security issues that may be barriers in sharing electronic health records.

One of the major challenges identified during the HISPC project was that organizations were hesitant to electronically exchange health information with each other because of mistrust due to the variation in their privacy and security policies. The Adoption of Standard Policies Collaborative was formed to develop an approach and process to identify and reconcile the variation in how organizational security policies are implemented across different electronic health information exchange models.[1]

This Adoption Guide outlines a process to define and harmonize minimum policy requirements specifically for authentication and audit and provides a framework to assist health information organizations (HIOs) as they seek consensus on privacy and security to support the exchange of electronic health information. The context for application of these policies is providers accessing patient health information for treatment purposes across HIOs.

Throughout this document the terms "minimum policy requirements" and a "Uniform Security Policy" have specific meanings, as follows:

- Minimum policy requirements are an agreed upon consensus set. They refer specifically to the policy requirements that the ASPC developed through extensive individual state review of current policy and the subsequent comparison and negotiation of these requirements across the 10 states in the collaborative. These minimum policy requirements become the framework across which the Uniform Security Policy was built. They are reflected in the Individual Requirements Review document, which can be found within the Final Report of the Adoption of Standards Policies Collaborative, located on the following website: http://www.okhca.org/providers.aspx?id=10202.
- The Uniform Security Policy is an aggregated set of policies that the ASPC recommends organizations adopt as a minimum policy to allow for interoperability with other organizations for health information exchange.

This document is the culmination of a 12-month effort to develop consistent common and minimum policies for authentication and audit. The states that participated in the ASPC were Arizona, Colorado, Connecticut, Maryland, Nebraska, Ohio, Oklahoma, Utah, Virginia, and

[1] Please refer to http://www.okhca.org/providers.aspx?id=10202 for detailed information about the process and work products of the Adoption of Standards Policies Collaborative.

Washington. Each state, through its governor's office, had the approval of the state government to participate in the Collaborative.

Additionally, many other policies and business practices that support exchange among organizations must be examined and because only 10 states and respective organizations within them were involved in this effort, further work remains to make the Uniform Security Policy applicable nationwide.

To define minimum policies for authentication and audit, the 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 included:

An environmental scan of existing best practice for authentication and audit policies and procedures, that included

- a review of literature and standards for authentication and audit concepts;
- a 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.

A negotiation of requirements for authentication and audit and policy development that included the following:

- 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.

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

The products the ASPC authored include the following publications:[2]

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

[2] The *Uniform Security Policy* is included as Appendix B 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.

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 ensure audit component compliance meant that timestamp needed to be communicated and stored to run a valid audit report. Another example is 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 led 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.

The following were concepts that were helpful in reaching consensus:

- 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 health information exchange 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 USP is offered as a best practice solution.
- Outreach throughout the process to stakeholders responsible for policy implementation.

While the goal of the ASPC was to define standard policies to achieve interoperability in health information exchange (HIE) on multiple organizational levels including statewide HIOs, state and regional HIOs, and HIOs in another state, this document will be pertinent to any exchange between any two entities. This adoption guide describes the process for working through and coordinating the efforts of several organizations as minimum requirements for authentication and audit are explored.

The Uniform Security Policy was developed to apply to any type of health information exchange architecture. Therefore, your organization's own experiences will be instrumental in building on the ASPC's initial experience and shaping the process for adoption into one that meets the unique needs of your state or organization. This adoption guide, along with tools in the appendices, should serve as a helpful starting point as security policies are developed.

1.1 Overview

The Adoption Guide includes the following sections:

Introduction

The Adoption Process

This section details a seven-step process for adopting the Uniform Security Policy. It includes information on gaining consensus from stakeholders and adapting the Uniform Security Policy to meet the unique needs of your specific organization and your state.

The following seven steps are described in detail:

1. Goal and Scope
2. Resources
3. Desktop Review and Risk Analysis
4. Consensus Building
5. Legal Assessment
6. Documentation of Policy
7. Implementation: Testing, Training, Deployment, and Production (including Evaluation and Maintenance)

Anticipated Challenges and Recommended Mitigation Strategies

This section provides an illustration of how HIOs that participate in health information exchange will benefit from adopting the Uniform Security Policy. It also provides a chart of potential challenges that can be expected during the adoption process, along with recommended mitigation strategies.

Summary and Next Steps

Recommendations made by the ASP collaborative are summarized and next steps are indicated.

Appendices

- **Appendix A: Feasibility—Preparing for Change and Process Checklist**
  An organization interested in assessing the feasibility of adopting the Uniform Security Policy must first be prepared for the significant changes that will be required to adopt and implement these standards. This appendix includes both a framework for preparing for change and a checklist to assist organizations in tracking progress of their implementation of the Uniform Security Policy.
- **Appendix B: Uniform Security Policy**
- **Appendix C: Other Useful Resources**
- **Appendix D: Glossary**
- **Appendix E: References**
- **Appendix F: Contributors**

1.2 Audience

The Guide is appropriate for both of the following audiences: (1) organizations that are just beginning their HIE efforts and therefore are adopting new policies, and (2) organizations that have HIE policies in place and that need to verify that their current policies, procedures, and practices meet the minimum requirements and possibly make some minor changes to what they already have in place.

This includes individual organizations (hospitals, health systems, health care providers,[3] and managed care organizations), HIOs, RHIOs, and state agencies (Medicaid, Health Departments).

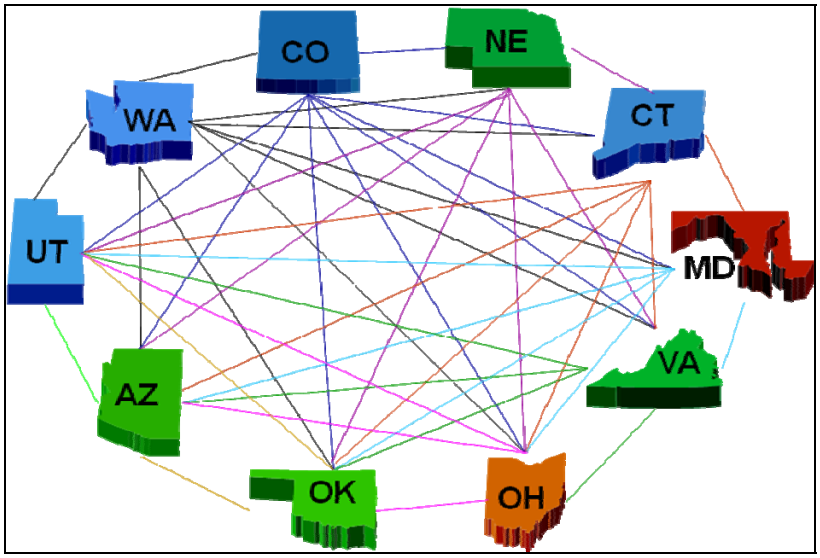
1.3 Purpose

The purpose of the Guide to Adoption of Uniform Security Policy is to provide support and guidance to entities as they review and adopt the Uniform Security Policy. The guide can be used to

- provide a framework for establishing inter- and intrastate authentication and audit policies through the use of minimum (core) policies that have been vetted by an interstate collaborative effort, and
- demonstrate how alignment of local policies with broadly accepted policies can facilitate health information exchange agreements.

With one-to-one policy agreements, each of the entities must negotiate with each of the other parties. The 10 states of the ASPC are illustrated in Figure 1-1. As the number of entities grows, the number of bilateral agreements grows almost exponentially; thus, for 10 states, there would need to be 36 bilateral agreements. Were one to consider all of the U.S. states and territories, the number of bilateral agreements needed would exceed 1,000, a daunting number of negotiations.

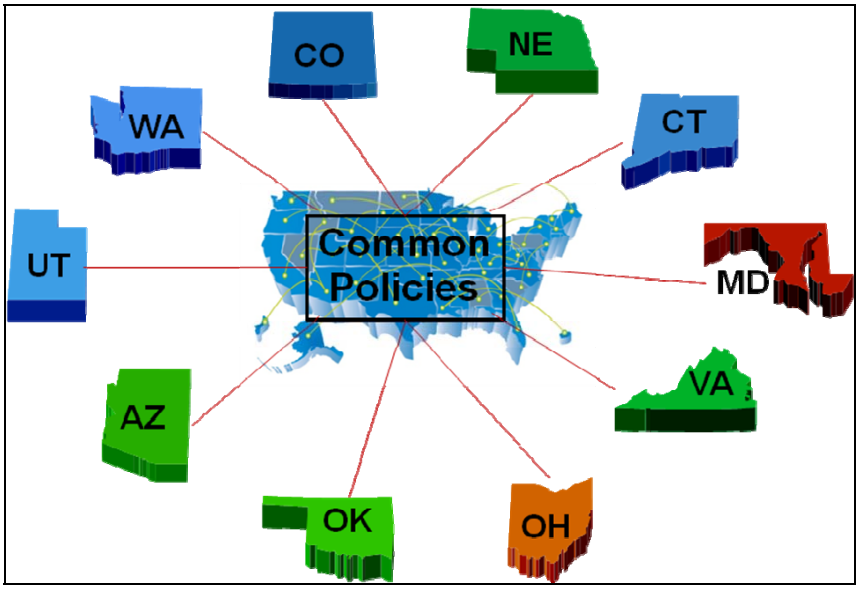
Figure 1-1. Problem



[3]The ASPC chose and used the definition of "provider" as given in the HIPAA Regulation, 45 CFR 160.103 and the privacy rule, 45 CFR 164.501.

Adoption of the Uniform Security Policy offered in this Guide to Adoption of Uniform Security Policy will create common policies for HIE by all the participants. To illustrate this benefit, consider that for the 10 states in the ASPC, the hard work of achieving consensus has provided the common policies (Figure 1-2).

Figure 1-2. Solution



1.4 Highlights of the Uniform Security Policy

In this Adoption Guide, a common policy, titled the "Uniform Security Policy" is recommended by the HISPC ASPC. This policy, which currently includes requirements for Authentication and Audit, has been publicly vetted and accepted and can be used to establish baseline privacy and security protections for organizations engaged in exchanging electronic health information for treatment purposes.

HIOs participating in HIE may have variations in security policies. Adoption of the Uniform Security Policy will help establish common business practices for registering and authenticating users, to benefit the individual users and the participating organizations. The guide will also help establish minimum audit requirements, consistent with the HIPAA Security Guidelines.

To successfully exchange health information electronically, HIOs must at least register, execute an agreement with, verify the identity of, provide digital identification for, and maintain an account for all users.

Each of these five processes has a set of minimal requirements that must be defined for HIOs to reliably trust their HIE trading partners and users and to be able to exchange health information with appropriate security rules in place.

The HIO must also consider the audit requirements for the HIE following the HIPAA Security Guidelines. The Uniform Security Policy provides minimum requirements for audit which include

1. logging and audit controls,
2. periodic internal compliance audit,
3. information access,
4. need to know/establish minimum necessary for data management and release,
5. need to know procedure/establish process for personnel access to personal health information, and
6. system capabilities.

Note:

- While the ultimate scope of a comprehensive security policy should include services that support operations and payment as well as treatment, the scope of the current Uniform Security Policy is specific to electronic authentication and audit policies and processes when a health care provider requests patient health information through an HIO **for the purpose of treatment**.
- The ASPC did not address the policies needed to govern provider authorization or access to specific types of health information permitted after the authentication process is complete. The project did develop the corresponding policies required to audit provider authentication as defined in the project. Because the audit policies considered both the authentication action and subsequent access to the records requested, the scope of the audit policies became broader.
- These policies do not necessarily pertain to the secondary use of data such as the exchange of data for the purposes of public health improvement or the detection and control of outbreaks; however, the process that the ASPC used to work toward common policies across the 10 states of the collaborative is likely to be generic enough to use as these other areas of data exchange are explored.
- The policy is determined as a minimum to be built upon. It can be more stringent depending on an organization's individual need and state-specific requirements.
- Throughout this document the term "state" is generic and includes any of the states, the District of Columbia, and/or territories of the United States.

Tables 1-1 and 1-2 list some key authentication and audit features of the Uniform Security Policy regarding use agreement, identity management, audit log data elements, audit reports, and enforcement.

Table 1-1. Key Authentication Features of the Uniform Security Policy

Use Agreement	Identity Management
• Information is true, complete, and accurate • Agree to comply with federal and state laws • Act in good faith and be truthful at all times • Access and use information only as permitted • Confidentiality, integrity, and accessibility will be reasonably ensured	• Unique identifier • Affiliation • Role

Table 1-2. Key Audit Features of the Uniform Security Policy

Audit Log Data Elements	Audit Reports	Enforcement
• Unique Universal ID of viewer • Role • Data elements viewed, created, modified, deleted, or transmitted • Date and time/duration of access	• Routine scheduled reports • Routine surveillance • Ad hoc reporting by request or on suspicion of inappropriate access	• Common policy on enforcement necessary for public trust of HIE, regulatory compliance and limiting legal risk

Benefits of the Uniform Security Policy include the following:

- Commonality *Across* States (because the Policy defines what is required in terms of the data set)
  - From a regulatory standpoint, it is important to adopt a policy set that supports systematic processes needed for ever-expanding HIE.
- Commonality *Within* States
  - Interstate exchanges can model their policies based on nationwide adopted standards.
- Starting Point for New HIOs
  - A starting framework for policy development would help any HIO as a floor for standardizing and develop consistent expectations prior to exchanging protected health information among organizations.

An outline of the Policy, including the focus of each section and subcategory covered, is presented in the following lists. The full Uniform Security Policy can be found in Appendix B.

Authentication

Section 1: Use Agreement
- 1.1 Requirement – Use Agreement

Section 2: Identity Registration
- 2.1 Required Data Set for Authentication
  - 2.1.1 Data Source
  - 2.1.2 Provider Identity Attributes

- 2.1.3 Organization Identity Attributes
- 2.1.4 Identity Attributes of the Data Source System

2.2 Role-based Access

- 2.2.1 Role

Section 3: Verifying Identity

3.1 Processes Used to Verify Identity

- 3.1.1 User Authentication
- 3.1.2 Organization Authentication
- 3.1.3 System Authentication

3.2 Variations Based on Type and Location of User

- 3.2.1 User Identity, Role, and Affiliation Verification
- 3.2.2 Signature Verification
- 3.2.3 Assurance Level
- 3.2.4 Relationship to Patient
- 3.2.5 Threshold Calculation
- 3.2.6 Digital Signature
- 3.2.7 Persistence

3.3 Accommodations for Cross-HIE Verification and Data Integrity

- 3.3.1 Restricted Data Sharing and Data Integrity
- 3.3.2 Authenticate Recipient Identity (Organization / System / User)
- 3.3.3 Required Elements for Matching
- 3.3.4 Matching Criteria
- 3.3.5 Digital Signature
- 3.3.6 Persistence
- 3.3.7 Data Authentication
- 3.3.8 Data Validation
- 3.3.9 Type of Requestor
- 3.3.10 Signature Purpose

Section 4: Identity Provisioning

4.1 Types and Levels of Provisioning

Section 5: Identity Maintenance

5.1 Registration Data

Audit

Section 1 – Logging and Audit Controls

1.1 Log-in Monitoring
1.2 Information Systems Review
1.3 System Review
1.4 Security Audit Practices
1.5 Audit Trail and Node Authentication (ATNA)

Section 2 – Periodic Internal Compliance Audits

2.1 Evaluation

Section 3 – Information Access

3.1 Audit Controls
3.2 Subject of Care Identity
3.3 Demographics that May Be Logged

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

4.1 Information Disclosure

2. THE ADOPTION PROCESS

To facilitate the adoption of minimum policy requirements for authentication and audit the following major steps and questions described in Table 2-1 should be addressed. The remainder of the Adoption Process section of the Guide will walk through each of these seven steps in detail. It is recommended you consult this checklist as needed throughout the adoption process.

Table 2-1. Checklist—Seven Critical Steps to Adoption

Step	Check	Questions Guiding the Interstate Process
1. Goal and Scope	☐	• What are the goals for this process? • What is the scope of the project; which use case will be used; what is the business model?
2. Resources	☐	• What team resources are required for this project? • Who are the stakeholders and what impact will adopting these policies have on them?
3. Desktop Review and Risk Analysis	☐	• Do you already have authentication and audit policies in place? • What business process are you trying to resolve? • How will you measure the risk associated with the business process?
4. Consensus Building	☐	• How will you build consensus among the team and stakeholders? • What specific methods will you use to achieve consensus? • How will barriers to consensus be addressed as you proceed?
5. Legal Assessment	☐	• How will you ensure legal requirements, including HIPAA guidelines, are incorporated into your policy? • Does your state have any laws that would dictate or affect the proposed policy requirements? • Do you need to work toward changing existing laws or introducing new legislation?
6. Documentation of Policy	☐	• How will you document the policy for end users? • How will you ensure that all policies are semantically accurate for digital translation prior to technical team implementation?
7. Implementation	—	—
a. Testing	☐	• How will you test that the software performs as expected, and only as expected? • How will you test the minimum policy requirements?
b. Training	☐	• How will you resolve issues that result from testing? • How will users of the policy be trained?
c. Deployment	☐	• How will you deploy the agreed-on minimum policy requirements?
d. Production	☐	• How will the implementation efforts be evaluated? • What are the outcomes to be measured? • How will you maintain the policy and ensure that it is not only adopted but also adhered to?

Note: Although these steps appear chronologically and as stand-alone, some steps may be performed simultaneously. For example, while defining your goals and scope, you may find that your team needs to have the appropriate resources in place to help with the goal definition process.

2.1 Goal and Scope Definition

The first step in the adoption of Uniform Security Policy is to establish a clear and realistic set of goals and to define the scope of the initiative.

Goals

Goals describe the end product that the health information organization (HIO) is trying to achieve. For purposes of adopting the Uniform Security Policy the goal would be to implement the minimum policy requirements needed to support health information exchange (HIE) between two or more states. If the organization is also going to adopt the Uniform Security Policy for use within the state, the goal should encompass that as well. The goal should be agreed on by all participating parties and should be distributed as a written document to which the team may refer at each meeting throughout the process. A clearly stated, common goal helps define the project scope (described below). As an organization develops the goal statement, consider the different models and sizes of participating HIOs, because this will impact the means by which organizations can adopt these policy requirements. For example, it may be unreasonable to expect a very small rural HIO to implement 2-factor or biometric authentication measures that a larger, urban and more-sustainable hospital has already implemented.

Scope

The project scope defines a common understanding of what is included in the project and what is outside the project. For instance, the idea of defining requirements for authentication and audit can encompass many different areas ranging from consumer authentication to auditing of system behavior. It is important to define the scope for adopting the minimum policy requirements for authentication and audit (and by extension, the Uniform Security Policy). Further, it is recommended that the scope include the context. For example, if an HIO decides the project will address provider access to the HIO for treatment purposes only, public health improvement or detection would be outside the project scope. The scope should clearly document the intent of the project and how the project will impact the key stakeholders. A well-defined scope increases the likelihood of attaining the goal and will help drive the business process analysis.

In identifying the scope of the project, there may be areas (such as authorization, access, and patient consent issues) which need to be included at a high level to complete some of the audit policy requirements. For example, when addressing the audit requirement of

knowing which provider accessed which patient's record, it would be necessary to understand how the patient was identified.

A strong scope statement for adoption of the Uniform Security Policy could be: "Analyze and define the authentication and audit requirements for a hybrid model HIO to use when allowing providers to access the HIE for treatment purposes, based on a medication management use case. " A very specific scope will help keep the project focused.

Role of Use Cases[4]

It is sometimes difficult to conceptualize what is involved in a process; therefore, it is recommended that "use cases" be included as the project scope is defined. These use cases are workflows that a specific system user would perform to obtain information. For example, an HIO may exchange laboratory data. The use case would document a description of an event and the actor who might need to be a part of the event. See, for example: **Sample 1: "Use Case/Business Requirements Analysis for HIOs Without a Current Security Policy,"** which outlines the method for defining a use case and how to proceed in mapping the use case to the minimum policy. Selection of use cases helps center discussion around which components of authentication and audit are essential to include as policy. The use case should apply to the planned organizational goal and should be pertinent to all the business models present in the HIOs involved. Spending an appropriate amount of time on each use case and organizational goals will be critical to facilitating the conversation between the business and technical teams within the organization.

Role of the Architecture of Business Models

The HIE business model includes the enterprise architecture in use, or planned for use in HIE, and is pivotal in determining the project scope. It is necessary to have a documented, detailed HIO enterprise architecture to determine the points in the system where authentication and audit are required. In the case of individual organizations, the same is true—it is necessary to document the detailed HIE structure that exists within an organization and between organizations. The architecture model may be one or a combination of several types of models, including but not limited to (1) centralized, (2) federated, (3) health record banking, and (4) hybrid models.

The model is used in conjunction with a use case to determine what policies should be required for authentication and audit. To reach consensus on minimum policy requirements, a state or organization with several HIE business models must be certain that all models are

[4] The Adoption of Standard Policies Collaborative (ASPC) found the AHIC use cases a starting point for our discussion, Although the AHIC were found to contain far too much detail for our purposes, the ASPC used the AHIC use cases to develop templates to capture the actors, actions, events and policy requirements pertinent to authentication and audit for each use case; and extracted the corresponding policy information from the AHIC use cases into the template. See the ASPC Final Summary Report at http://www.okhca.org/providers.aspx?id=10202.

accommodated. Many states will want to work with other states to define minimum policy requirements and in that case, each state should be prepared to document its business model or models to perform use case mapping that then becomes the basic policy requirements.

2.2 Resource Planning

Team Resources

In addition to time and material resources, human energy and activity are required to perform the business process/use case mapping and analysis to determine the recommendations for adopting the Uniform Security Policy. Recommended resources for adoption include a project manager, business analyst, security analyst, technical support, legal counsel, and episodic availability of stakeholders. This team would be responsible for bringing the project to a successful conclusion, and ensuring consensus among stakeholders. It is important to invest in having the correct resources and to continually evaluate these resources as the project matures, to ensure that they are available and devoted to supporting the adoption of the Uniform Security Policy.

Stakeholders

How to Involve Stakeholders

Stakeholders might be asked to participate in a working group and meet on a monthly basis to help review and evaluate the Uniform Security Policy. Assignments for this group would include use case mapping, documentation of standards, and detailed review of the minimum policy requirements for authentication and audit. The recommended approach is to provide the stakeholders with the goals and scope as well as the detailed schedule, outlining when input will be expected and what type of input will be needed from them. Since the stakeholders will have a vested interest in how these policies work, it is important to include them in major decisions around the adoption of the minimum policy requirements. A Steering Committee or other review body will take the work completed by the working group and approve the policy implementation. A steering committee would be composed of high-level stakeholders, such as those from leadership and managerial ranks from the medical community mentioned above. This group could meet monthly or quarterly to review the progress and results from the efforts in adopting minimum policy requirements for authentication and audit. Having “buy-in” from this group is important to success overall, as they, too, can become advocates for the results.

Organizations from which community stakeholders may be drawn include the following:

- hospitals and hospital associations,
- medical groups,
- schools of medicine/osteopathy/nursing/pharmacy,

- medical association chapters (for example, of the American Medical Association),
- behavioral health organizations,
- state and/or local health care and public health departments and agencies,
- community health center representatives,
- quality improvement organizations,
- health/managed care plans,
- forming or existing HIOs,
- local sections of the Healthcare Information and Management Information System Society (HIMSS),
- advocacy groups (for example, the American Association of Retired Persons),
- law offices specializing in health law,
- consumers, and
- employers.

Participation of various stakeholders in analyzing and reviewing the authentication and audit minimum policy requirements is critical to the success of the adoption process. Not only should stakeholders be involved in setting new policy, they should be involved in adopting an existing policy. This will ensure broad consensus as you move forward. Representation from the community and a diversity of disciplines is recommended to achieve consensus.

2.3 Desktop Review of Business Processes and Risk Assessment

Desktop Review of Business Processes

To determine whether the Uniform Security Policy is going to be adopted by your organization, it is first necessary to perform a desktop review of the business process the authentication and audit will apply to. Each component of the Uniform Security Policy needs to be reviewed against each actor and event applicable to the business process.

Step one in the business analysis process is to use the selected use case to define the actors, the information they would need to access, and the authentication and audit requirements. If specific policy requirements are not in place, the use case can help define what policies would be needed for a specific use case and business model. If there are existing policy requirements in place, these can be used as a comparison tool to determine whether the Uniform Security Policy can be adopted. If policies for authentication and audit do not exist, it is necessary to analyze the business requirements for providers accessing the HIO for treatment purposes. The first step in this analysis is to determine who the actor is that will be processing transactions through the HIO for the use case selected. It may be necessary to reiterate that the basic minimum policy requirements are only for providers accessing the HIO for treatment purposes. This method of analysis can be used to

determine the business process requirement for each person accessing the HIO and the patient information that person would need to access. The business requirement is compared with the authentication and audit requirement to validate that this is a point at which the actor would need to be authenticated and subsequently, audited.

The sample below illustrates how this process would work, citing a portion of the applicable security policy element. Some Uniform Security Policy statements may require more than one test scenario. For example, Appendix B, Section 3, element 3.1.1 addresses the registration of the provider and the authentication method. It is necessary to test each of these elements individually.

Table 2-2. Sample 1: Use Case / Business Requirements Analysis for HIOs Without a Current Security Policy[5]

Actor	Event	Authentication / Audit Requirement	ASPC Recommended Basic Policy Requirement	Issues	Resolution
Clinician	Laboratory results for a patient	Clinician is identified by the trusted authority Clinician logs into system using password and login name	**Authentication Section 3 – Verifying Identity** 3.1.1 User Authentication 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).	Current system only allows for password	Upgrade system security to allow for shared secret
HIO	List and review of people accessing the HIO	HIO must be able to audit access to the HIO by providers	**Audit Section 1 – Logging and audit controls** 1.1 Log-in Monitoring Audit log is required and must be reviewed on a regular basis.	No issue	NA

Once the business process analysis is completed, issues should be discussed with the team and the stakeholders. For example, if a “shared secret” is the business requirement, any HIO participant system that does not provide for a “shared secret” as part of the authentication process will need to determine how to provide this functionality, for those who want to exchange with other HIO participants.

[5] The authentication/audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

The next step in the business process analysis is to map the future requirements for authentication and audit to the business model defined in the project scope, using the selected use case(s). This can be accomplished by constructing a flow chart of the relevant HIO architecture and identifying points at which authenticating a user or system, or auditing access to the HIO should be conducted, based on the use case. The mapping of the use case to the system architecture will confirm that all the authentication and audit requirements for secure transmission of medical data have been identified.

If there is already a security policy in place, a desktop review of business requirements analyses can be performed by comparing policy requirements within the Uniform Security Policy with the organizations existing security policies. Existing security policies might be entity specific (i.e., your hospital's policies, HIO policies, policies associated with a particular business model or state agency, policies that pertain to a particular application like an immunization registry). The purpose of the desktop review when an existing policy is in place is to check for gaps and propose recommendations to adopt the Uniform Security Policy. The desktop review can be completed by using the following format to track and compare your local policy requirements with the minimum policy requirements in the Uniform Security Policy.

Table 2-3. Format for Business Process Analysis for Organizations Having a Security Policy[6]

Uniform Security Policy Requirements	Local Policy	Gaps	Recommendation	Solutions
Authentication Section 1: Use Agreement 1.1 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 users' method of connection and the sensitivity of the data that will be exchanged.	Local one-to-one contracts	Stricter than minimum	Accept a less strict policy for cross-state sharing only	Allow for cross-state sharing of HIE

[6] The authentication/audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

Uniform Security Policy Requirements	Local Policy	Gaps	Recommendation	Solutions
Authentication Section 2: Identity Registration 2.1 Required Data Set for Authentication A directory of data sources within the target HIO is required, and includes primary contact information of registered members, identity attributes of providers, organization, and systems.	Same	None	Accept minimum policy requirements	
Authentication Section 2: Identity Registration 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.	None	Currently no such data source	Need new system capability	Install and deploy new system capability
Authentication Section 2: Identity Registration 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. Required elements are profession, role, name, practice address, business/ legal address and License/ID.	Required but no field in the system for role	Roles not codified and assigned	Add field for role	Update application

Once the desktop review is completed and gaps and/or issues have been identified in the authentication and audit process, a risk analysis should be completed. It is also possible to begin the risk analysis during the desktop review process.

Risk Analysis

A risk analysis should be performed when adopting the Uniform Security Policy. This assessment will be critical in determining what threats and vulnerabilities may impact the users and systems and what security controls have been implemented to protect against identified threats and vulnerabilities. The risk analysis can be performed at the inception of

this process as the desktop review is being completed. A risk analysis should also be completed whenever a significant business or technical change occurs following implementation. This assessment involves reviewing the data, hardware, people, and networks; and prioritizing those items and determining what threats and vulnerabilities exist, what security controls are already established and where action may be necessary to prevent regulatory, liability, financial and reputation issues. Further, the risk assessment will help define the type of audit reports you need to have and the type of monitoring requirements you need in place. The risk assessment should be done in relationship to the Uniform Security Policy.

The following steps should be followed when conducting a risk assessment of an HIO:

- definition of system boundaries;
- system inventory (hardware, software, facilities and data);
- identification of information owners (electronic and nonelectronic data);
- identification of workforce members with access to stored data by hardware/software;
- mapping data flow and identifying data exchange points (e.g., where data are transmitted from one system to another, from the system to an individual or entity, etc.);
- conducting an inventory of data storage (including nonelectronic data);
- assessment of criticality (for example, mission critical, important, ancillary, etc.);
- vulnerability identification;
- threat identification;
- security control analysis using the Uniform Security Policy;
- likelihood determination (for example, how likely will an identified threat or vulnerability impact the organization given existing security controls);
- impact analysis (for example, what is the cost if an identified threat or vulnerability impacts the organization given existing security controls);
- risk determination (based on likelihood and impact);
- security control changes/mitigation recommendations; and
- results documentation (includes mitigation plan and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost).

Please refer to the National Institute of Standards Technology (NIST) 800 series of publications on this topic to complete a risk assessment (http://www.nist.gov/index.html).

2.4 Consensus Building

After each HIO within a state or across state lines has mapped the recommended basic policy requirements to the individual models, negotiations with the project team and stakeholders may be necessary to reach consensus about the adoption process. Conflicts may be inevitable but can also be productive in the negotiation process. In a negotiation process, it is important to have a neutral facilitator who will manage all meetings during the negotiation process (e.g., setting meeting schedules, keeping minutes, and tracking both policies agreed upon and areas that require further negotiation). The facilitator should have the knowledge and skills to articulate differences in the types of authentication and audit, be an experienced facilitator, and bring the group to consensus about which will work as a basic minimum policy requirement. It will be important to emphasize the positive elements of adopting this policy; for example, the value of having a Uniform Security Policy in place will enhance an organization's ability to exchange electronic health records. The legal considerations should be highlighted and discussed as well so there is an understanding of legal compliance. It will also be important for each stakeholder to understand the impact of the policy on other stakeholders. For example, a provider will have a different view of what should be audited than a consumer.

The following should be taken into consideration at the consensus building phase:

- Documented desktop review of business processes for each HIO represented should be available.
- Appropriate personnel including the business analyst, security analyst, and technical support should be included.
- A decision maker who has the authority to make decisions about the policy in case of negotiation should be included in any negotiations.
- Issues will need to be tracked as "parking lot issues" and resolved before the policy analysis is complete.
- It may be necessary to involve the legal counsel as negotiations progress to be sure any state or federal legal requirements are taken into consideration.

The following are some techniques commonly employed by organizations to achieve consensus and improve group decision-making. A brief definition is included below to describe each technique and each will involve several steps that reference how to successfully execute the method.

- **Delphi technique**: This technique collects and uses opinions of individuals with certain expertise by mail. Responses are ranked, compiled, and computed. The consensus is used to make a decision. This would involve listing the items from the policy that you are unable to reach consensus on, providing the detail around those items and collecting responses for ranking.
- **Nominal group process**: This technique involves small groups of individuals who systematically present and discuss their ideas before privately voting on their preferred solution. The most preferred solution is accepted as the group's decision.

- **Stepladder technique**: This technique may be used to minimize the tendency for group members unwilling to present their ideas by adding new members to a group one at a time and requiring each to present ideas independently to a group that already has discussed the problem at hand. [7]

2.5 Assessment of Legal Requirements

Integral to the adoption of standard policies is a complete legal review of HIPAA, other federal laws (such as CLIA regulations and federal substance abuse treatment regulations), and relevant state statutes and regulations. Given the complexity of legal requirements that affect security policies for HIE, it is important to include legal expertise during the process of adopting these minimum policy requirements for authentication and audit. Although HIPAA and other federal regulations were taken into consideration in drafting the Uniform Security Policy, adopting states should review their own state laws that may impact the adoption process (and should keep abreast of federal laws issued after the date the policy was issued).

The legal review should be completed once the use case has been mapped to the model architecture, because legal requirements for authentication and audit may change with different HIE architecture and use cases (who will have access to the information and for what purpose). In addition to considering federal and state laws that apply in the adopting state, the legal review should encompass ways to minimize legal risk in the policy. Many states tie these requirements to HIE participation agreements as well, to require HIE participants to comply with the applicable policies.

Once the legal review is completed, the team should give serious consideration to any legal issues that may hinder the adoption of the minimum policy requirements. At this point, it may be necessary to return to the desktop review phase and reconsider some of your recommendations. Or, you may need to go back to the consensus-building process and get buy-in on the changes required as a result of the legal review. Alternatively, it is possible to go back to the state legislature and get statutes changed or work with the appropriate state agency for rule/regulation amendment.

If your state is considering interstate exchange with other states, consider conducting the legal review with representatives from the other states to facilitate identification of different state laws (or different interpretations of federal laws) that may pose barriers to exchange.

2.6 Documentation of Policy

After the legal review and final negotiation of policy are complete, the policy should be documented not only for the end users but for the technical team. The Uniform Security Policy should be documented as it applies to the organization. It is important to ensure that the written policies agreed upon can be understood by the users and the technical team.

[7] Greenberg, J., and Baron, R. (2007). *Behavior in organizations*. Upper Saddle River, NJ: Prentice Hall.

At this point it will also be necessary to document the configuration of existing applications. This will ensure that the written policies can be executed with your applications. This means that special care must be expended in drafting the specifications that are passed to the technical team that will be configuring appropriate applications, customizing those applications, or developing the needed applications. Because of the sensitivity to unauthorized disclosure of protected health information (PHI) and the compliance rules of which the HIO must be aware, this is an important step in the process. The technical team will need specific instructions to implement solutions that do not permit illicit activity. By careful drafting of the application specifications, this type of activity can be avoided. The implemented applications will do what is expected, but no more. An example of this type of specification follows:

Table 2-4. Sample Technical Specification of a Policy Statement[8]

Policy Statement	Technical Specification	Date Completed	Issues Reported
Authentication Section 2 -Identity Registration 2.1.2 Provider Identity The HIO will collect the attributes as needed for unique identification of the individual accessing the information in the HIO. Required elements are profession, role, name, practice address, business/ legal address, and License/ID.	Coding must include a role.	Ex. 2-27-10	Custom code required to add field for role.
Audit Section 6 – System Capabilities **6.4 Data Authentication** For purposes of data authentication the use of a valid date/time stamp is required.	Coding of the system and the audit reports must include the valid date/ time stamp required. Date stamp needs to print on the audit report.	Ex. 3-5-09	Audit report does not include time of access.

[8] The authentication/audit requirement in the sample contains one element of that requirement. Refer to the full Uniform Security Policy in Appendix B for all elements.

2.7 Implementation

The implementation phase of the adoption process includes the following:

- **Testing**—functional, regression, system, integration, and load testing;
- **Training**—training the end users and the support team;
- **Deployment**—deploying the new policy to the end users and the systems; and
- **Production**—post implementation review, modification, and support.

2.7.1 Testing

The testing phase is critical to the successful adoption of the Uniform Security Policy. Testing of the new policy against the applications is completed so that the users can determine whether the new policy is going to satisfy requirements for using the system from a security viewpoint. It is important that testing validate that the system is responding as expected to the new policy; however, it is more important that users can abide by the new policy and that the user's work load is not increased.

Preparing to Test

The purpose of testing is to determine whether the Uniform Security Policy and technical requirements of the policy will operate as planned within a given organization's technical environment. It is critical that test scripts are developed to reflect the use case and workflow as well as the authentication and audit points that are required based on the basic minimum policy requirements and the work completed in the desktop review of business processes. Having formal test scripts will help track areas where gaps may be present or identify any type of system malfunction that occurs while testing the policy.

As you are preparing for the testing phase, it is important to develop test scripts that reflect the workflow expected with the Uniform Security Policy. They can be used for each testing phase and should reflect the actual workflow that the HIO performs. The test scripts can be developed by determining the action a user or (actor) would perform based on the policy element from the Uniform Security Policy. Each element in the policy needs to be tested. Below is an example of how a test script should be designed. This example reflects adding a provider to the system and authenticating the provider.

Table 2-5. Sample 4: Test Script Sample—HIO Entering Provider Data[9]

Script Number	Test Script Name/Policy Reference	Action	Actor	Expected Results	Issues
1	Identity Registration: ref. 2.1.2 Provider Identity Attributes	Add a new provider to the system, using the required attributes: profession, role, name, practice address, business/ legal address and License/ID	HIO	Successful addition of provider to the system, issuance of login and password	None
2	Verifying Identity: 3.1.1 User Authentication	Provider is accessing lab results using login and password	HIO	Provider uses assigned login and password to access the system	Provider unable to login in; fix and retest

It is critical to also have a list of standard data that the testers will use in their testing. (This list will likely grow over time as more use cases are added.) A sheet of allowable attributes for testing can be developed to be referred to depending on the script. It is required to have data for each test script. Using predetermined data for entry gives the users and the technical team the ability to track those data through the system, validating that the data went into the right fields and show up on the audit reports. It can also help when debugging the system. Table 2-6 is an example of predetermined data.

Table 2-6. Sample 5: List of Provider Data for Testing for Script #1 and #2

Profession	Name	Role	Address	Business Address	License #	Test Login	Test Password
MD	Dr. J.	Provider	6 Oak Street	6 Oak Street	123456	Drj	Drjej!23J34*
PA	Tim Jones	Physician Assistant	8 Tree Street	8 Tree Street	123454	Timj	DF$c56J23#

The database and applications must be configured to reflect the Uniform Security Policy prior to testing. The application specifications provided in the Documentation of Policies

[9] Each element of the Uniform Security Policy components must be tested. There may be more than one action in (for example) authentication policy 2.1.2.

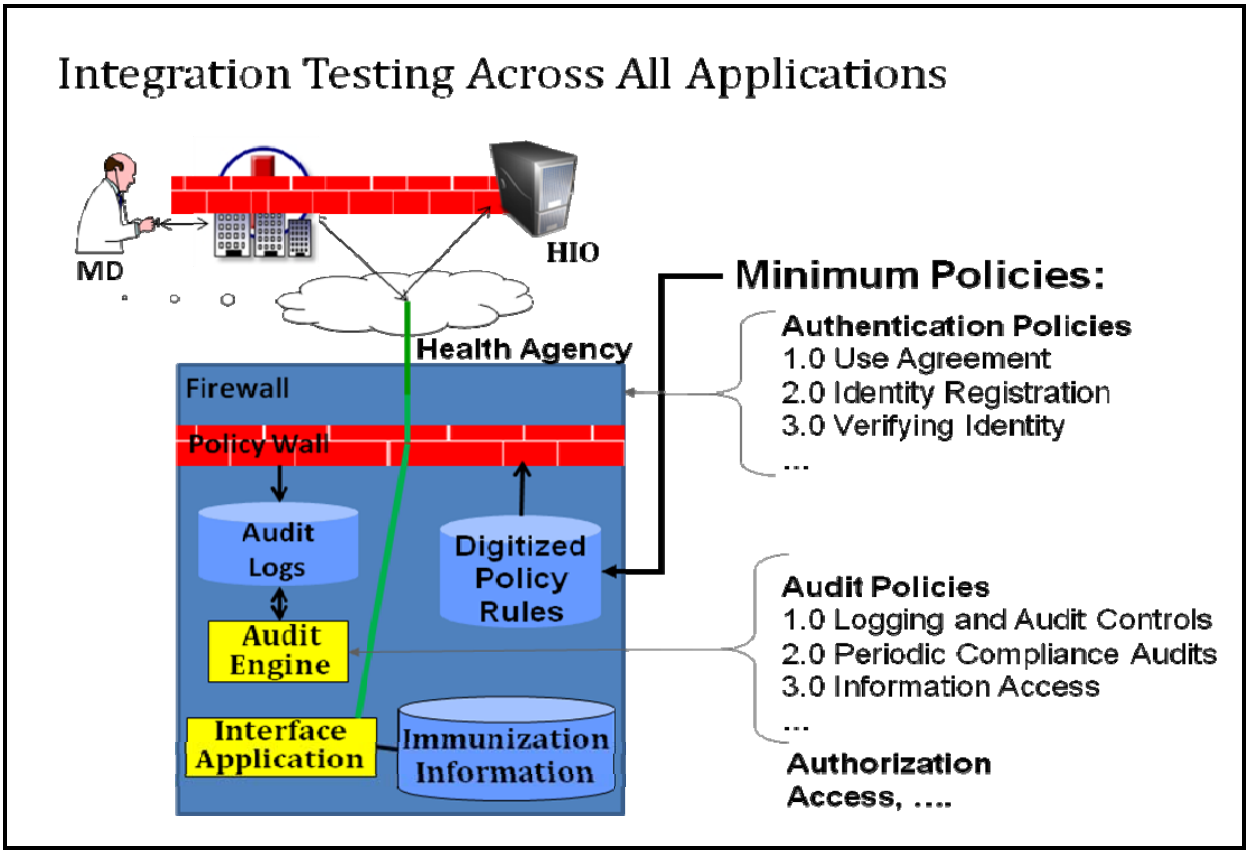
section provides the basis for the technical work. This can be done using configuration methods but in some cases may require custom coding. The process involves converting the policies into digital rules on a test database that should be a replica of existing HIE database and applications.

Important note:

Because testing involves many different types of users, it is critical to de-identify the data used for the test to protect patient identity. Testing should also be limited to a test environment using valid logins and passwords that apply only to that environment.

Figure 2-1 is a graphical representation of policy integration. As a transaction enters an organization's system, it typically passes through a "firewall" that provides an initial security screening. Policies need to be digitally implemented in the next layer of security, a policy rules engine or "Policy Wall." Basic policies (written in English) are converted to Digitized Policy Rules which are parsed according to the type of transaction and implemented with a minimum amount of human intervention. The authentication policy invoked by a particular type of transaction should determine the success or failure of passing through the Policy Wall. Both incoming and outgoing transactions should pass through the Policy Walls rules checking. Because the audit policies are meant to record activity "after the fact," they are not intended to be an upfront screen function. However, it is necessary to ensure that the correct information is being recorded.

Figure 2-1. Testing of Applications and Infrastructure



Next are the five levels of testing that should be completed while evaluating adoption of the Uniform Security Policy. A description of each level of testing follows:

1. Functional Testing
2. Regression Testing
3. System Testing
4. Integration Testing
5. Load Testing

Functional Testing

The first phase of testing the Uniform Security Policy is the functional testing. This should be completed to prove that the system configuration for the security policies is working on each individual software application. For example, if there is a Master Provider Index, a test would be completed on that application to ensure that the test script for entering provider data is validated and in the system. Information entered into the fields in the Master

Provider Index should be checked to confirm it is the expected result. The process should be completed for each application in the architecture.

Regression Testing

Within the testing phase regression testing proves that the system does not work when it should not work. An example of this would be to prepare test scripts knowing that the data for adding a provider to the system are missing an attribute. For example, the Uniform Security Policy requires that the provider license be entered into the system when you register the provider. This testing phase would purposely leave out the license number for a provider during the data entry. The result should be that the system does not accept that provider. The tester will enter the data he or she does have for the provider and the expected result is an error message "all fields are required, provider entry cannot be completed." To validate this error, check the Master Provider Index to make sure the provider did not get entered into the system. Regression testing should be completed at each phase of the testing.

System Testing

System testing is the testing of the database and applications within the HIE of the Uniform Security Policy. This phase of testing is still at the organization level and tests the workflow for a provider accessing a patient record for treatment purposes all the way through the system, touching each application as required to prove that the Uniform Security Policy will work throughout the applications. The same test scripts from the functional test can be used; however, each application must be checked to validate that the provider data are where they are supposed to be and that the authentication of that provider works as the Uniform Policy states. The auditing process should be checked thoroughly during this phase as well. Once all the test scripts have been completed, audit reports should be generated and checked against the test scripts to be sure all applicable information is on the audit log. Again, the audit reports should reflect the components of the Uniform Security Policy. Any and all issues should be resolved before moving into integration testing.

Integration Testing

Integration testing occurs after the system testing. This is the testing where the HIO is validating that all interfaces to external or internal systems are working properly based on the Uniform Security Policy. Integration testing involves the test of sending transactions that relate directly to the Uniform Security Policy, between multiple applications and/or organizations to determine whether interfaces work, the data transmitted are what is expected, and the established policies are supported as data move between organizations. Because these policies are meant to apply to sharing of electronic health information across state lines, it is necessary to have any partner HIOs involved in the testing process. The check points tested include adding a provider, authenticating that provider, and providing

an audit record of what the provider accessed and when. Again, all of this is based on the Uniform Security Policy and a test script should be developed for each policy element.

The methods for testing in the system test also apply to the integration testing. Both methods of testing need to ensure that each use case transaction invokes the proper policy rules at the appropriate level of testing. Any issues that are found should be classified by type of issue and resolved by reviewing and modifying the workflow, the software, and the hardware functionality or the policy.

Once the issues have been resolved it is necessary to completely test the system and the integration until you can get through all your test scripts with all issues resolved. At that point it is appropriate to move to the next phase of testing.

Load Testing

Load testing is the testing of the system to examine scalability issues. This type of testing is done to ensure that the software applications will be able to handle the normal workload, with the Uniform Security Policy in place. Load testing is completed by using the test scripts already developed and having several people perform each transaction at the same time. If the system becomes slow, it may be necessary to tune the database and/or have a hardware review. At this point the technical team may also need to review the policy configuration or the custom coding, if applicable.

As a final step, the testing team needs to document that all testing was successful. This documentation will be important for Certification and Authorization to operate using the Uniform Security Policy. The documentation should ultimately be approved by the project team and stakeholders.

2.7.2 Training

Creation of a training plan is an essential step in ensuring properly implemented Uniform Security Policies for authentication and audit. The plan should reflect system roles and access requirements, define users, and document functionalities of the system and how they integrate with subsystems, because this relates to the Uniform Security Policy. The plan needs to identify who will be trained in what role level, what methodology and curriculum will be used, who will conduct the training, how frequently the training will be repeated, and how the training will be evaluated. Ongoing training beyond “go live” should be offered whenever the authentication and audit policy changes, a new application and/or HIO is added, or new system users are brought on board.

Initial feedback from the stakeholder group should be included in the design of curriculum and care should be taken to have the curriculum reviewed by the privacy, security, and legal professionals assigned to the team.

The training plan should include the groups targeted and standard messaging about the organizational minimum policy requirements. It is critical that all training materials be consistent across all HIOs with emphasis on the group you are targeting. HIPAA and other applicable federal and state laws should be included in the training materials so everyone is aware that by adopting the Uniform Security Policy, regulatory requirements have been addressed and are being adhered to.

To ensure transparency and public "buy-in" for the project, it is recommended that a structured public education/outreach effort be undertaken with the following groups:

- **State Government**—State government should be informed about the HISPC at a high level with emphasis on the Adoption of Standard Policies Collaborative and the basic minimum policy requirements around authentication and audit.
- **HIOs**—The detailed basic minimum policy requirements and the Uniform Security Policy should be shared with all HIOs and adoption should be encouraged so they are able to effectively achieve interoperability with other HIOs.
- **Provider Community**—The provider community will need to be aware of the Uniform Security Policy and how it will impact them. It is recommended that the HISPC Provider Education Toolkit be reviewed as a tool to help make providers aware of these policies.
- **Consumer Community**—The Uniform Security Policy should be shared with consumers so they can be assured that their health information is protected in a consistent, safe manner.

2.7.3 Deployment

Once system testing is complete and the system users have been trained, it is time to deploy the Uniform Security Policy. The following steps should be taken during the deployment phase:

1. Determine a "go live" date for the Uniform Security Policy across HIOs.
2. Complete and document the training phase with all system users.
3. Ensure that all new or modified applications (off the shelf or custom programmed) to accommodate the Uniform Security Policy have been installed and correctly tied to the production database by having the technical team document new or modified applications that need to be moved into the production database and creating a checklist to follow.
4. Have the appropriate support in place to handle questions that may arise with the use of the Uniform Security Policy. For the first week or two it may be necessary to have additional staff on your support team to ensure fast response times for systems users. This support team should be a combination of business analysts and technical personnel.
5. Communicate the "go live" to the system's users, provide copies of the policy and a documented support mechanism (this could be your "help desk" procedure).
6. Post copies of the policies and user guides to each organization's intranet or colocate them on a common secure website.

7. As users begin using the system and the new policy requirements, keep track of any issues that may arise.
8. Regularly review issues and make modifications as necessary to training material, FAQs, policy verbiage, and other supporting material.
9. Regularly schedule follow-up/refresher training for all users required to adhere to the new policies.

2.7.4 Production

The production phase involves the actual "go live" and the ongoing evaluation and maintenance of the Uniform Security Policy. The first item that should be addressed at "go live" is the support requests received from your users. These requests can include many different types of issues. Many times when a user needs support, it can be attributed to user error, system error (bug), and/or a workflow process. The support requests should be continually evaluated and may require decisions around several areas. Some of the questions to ask when reviewing support requests follow:

- Is the workflow efficient when using the Uniform Security Policy? For example: Is the authentication practice efficient for a provider to use during a patient encounter? Should business process analysis be completed again?
- Are there software bugs in the application when implemented in a production environment and/or integrated with the production database? Remember: A system and/or integration testing must be completed again after the bug fix is applied to the test database. You may find that users have workflow that will need to be added to the test data.
- Was training sufficient for the users? Are there groups or sub-groups of users that need more instruction on the policies, procedures, and/or practices? Should the training material and the material posted on an organization's intranet site or common website be revised?

In addition, the HIO should have answers to the following questions regarding the production phase:

- How will you measure the successful application of policies after they are moved to production?
- How will you evaluate on a regular basis if the policy is current and/or needs to be modified because of regulatory changes, changes in the environment, technical changes, etc.?
- Who is responsible for policy updates, ongoing monitoring for effectiveness, and follow up training, especially when policies change?

By keeping track of the support requests, the HIO can begin to measure the effectiveness of the adoption of the Uniform Security Policy. It is possible to create reports that can show the types of issues encountered, who encountered the issue, the response time to resolution, and improvements in system use. This will be very valuable as the effectiveness of the adoption process is measured.

It is important to have a process in place to continue evaluating and maintaining the usefulness of the Uniform Security Policy because the policy may be impacted by several issues. It is suggested that the steps in this adoption guide be used to evaluate the Policy if any of the following events occur within your organization:

- addition of any new business process to your workflow,
- a change in workflow,
- an upgrade of your software applications,
- an upgrade to your hardware infrastructure,
- results from regularly conducted risk analyses and compliance audits, or
- a change in federal or state law related to privacy and security.

3. ANTICIPATED CHALLENGES AND RECOMMENDED MITIGATION STRATEGIES

As depicted in Figure 3-1, the focus of health information exchange is the secure transmission of meaningful health data across organizational boundaries. The legal and policy context of health information exchange is found in federal rules and laws that are further modified by state laws. The technical foundations for secure and private transport of health information are principles used to control the "4 A's":

- **Authorization** (who gets to view and edit the data)
- **Authentication** (how we know them to be who they assert)
- **Access** (what data they can access)
- **Audit** (the record of who has seen and changed what data)

The applications of the principles outlined by the 4 A's are specified in legal agreements among organizations, health information exchanges, and the Nationwide Health Information Network. This network of trust will benefit from the Uniform Security Policy recommended by the Adoption of Standard Policies Collaborative.

Figure 3-1. How Health Information Exchange Fits in the Legal and Security Context

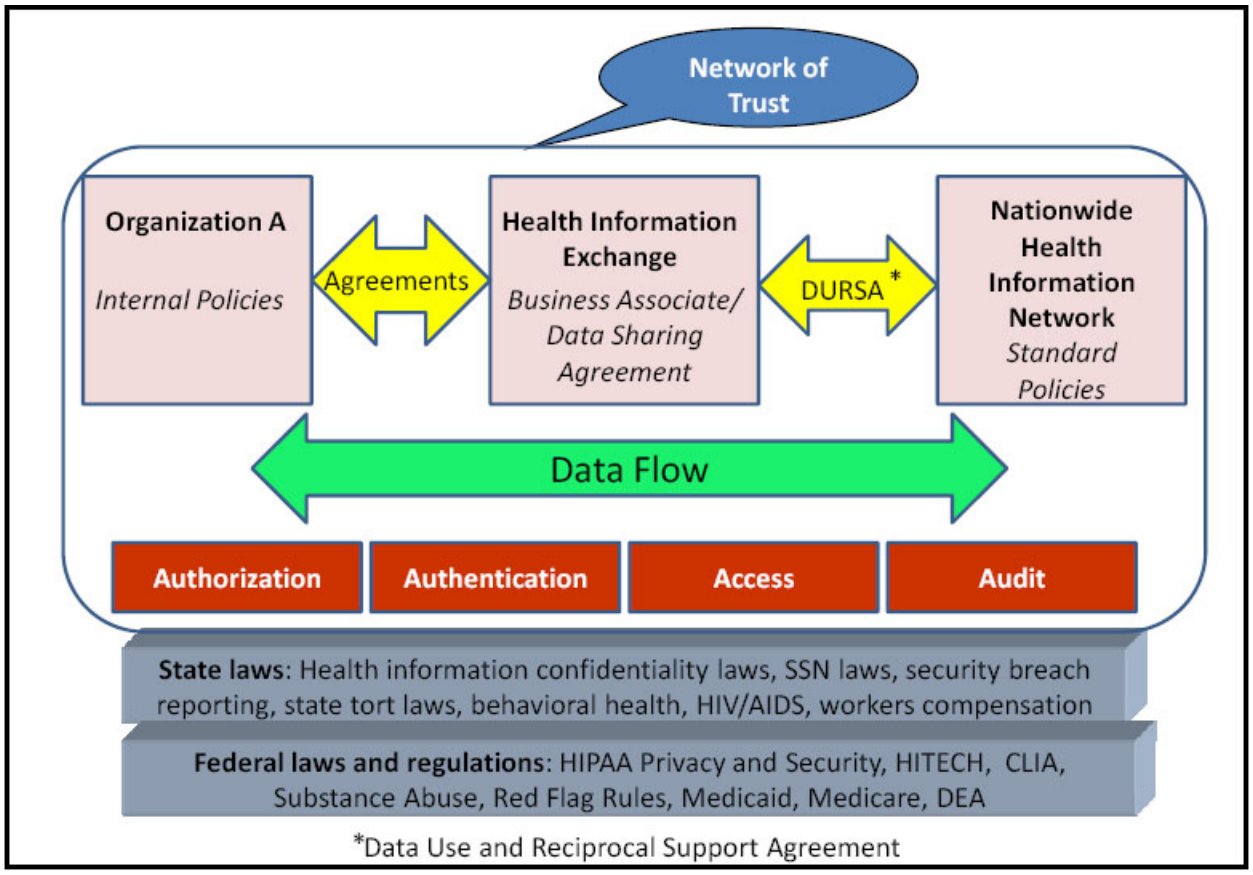


Table 3-1 delineates some anticipated challenges that your organization may face during the adoption process and some potential mitigation strategies to effectively address these categories.

Table 3-1. Anticipated Challenges and Recommended Mitigation Strategies

—	Anticipated Challenge	Mitigation Strategy
Business	Local or regional solutions do not conform to national standards	Educate member organizations on standards and the benefits of standards.
Business	Nomenclature varies across organizations	Use the technical work group to map nomenclature to the standard.
Business	Funding is not available	Write the business plan; solicit funding.
Business	National standards have not been adopted	Review draft national standards and coordinate local/regional standards development to match, where feasible, draft new national standards; inform national standards organizations of lack of standards.
Business	Administrative, physical, and/or technical safeguards are not adequately addressed	Incorporate regularly scheduled and comprehensive review of policies, procedures, and practices into the business plan. Regularly schedule risk analysis and audit (periodic and compliance). Provide regular training to new and existing users and management.
Legal	Granularity of audit logs is not adequate for reports	Evaluate system triggers; implement more granular data capture.
Legal	Too many or too few audit logs are generated but do not capture either what is needed or more than can be reviewed in a timely manner	Perform a legal review of audit plans and procedures and proposed content of logs to reduce legal risk, meet appropriate security standard requirements, and address regulatory requirements.
Legal	Identifying data specified in policy: • Behavioral health • HIV/AIDS • Sexually transmitted diseases • Alcohol and chemical Dependency • Worker's compensation • Medicaid • Medicare • Certain minor information • Genetic • Reproductive	Establish a legal work group to review policies, law, and practices related to consent, authorization, and specific "more stringent than HIPAA" requirements.

(continued)

Table 3-1. Anticipated Challenges and Recommended Mitigation Strategies (continued)

—	Anticipated Challenge	Mitigation Strategy
Political	Lack of transparency	Educate the stakeholders; develop a website for documentation and dissemination.
Political	Assumptions are not clearly defined	Improve governance processes to include better communication and greater specificity.
Political	Complaints of lack of inclusiveness from stakeholder groups	Widen reach by adding more stakeholders. Communicate with stakeholders who had been invited to participate and elected not to be involved, reinviting them to the table.
Technical	Varying authentication practices	Define the minimum requirements by adopting the standard policies.
Technical	System performance/ scalability	Provide a technical evaluation of changes recommended to effect improvement including resources and timeline.
Technical	Identifying data specified in policy: • Behavioral health • HIV/AIDS • Sexually transmitted diseases • Alcohol and drug • Worker's compensation • Medicaid • Medicare • Certain minor information • Genetic • Reproductive	Present a list of all available data elements to have reviewed by legal. When feedback is provided implement the ability to "lock"/ "unlock" data elements by role.
Technical	Legislation or regulations are required to implement the policy	Identify models and educate the lawmakers and/or regulators.
Educational	Policy implementation requires legislation or regulation	Prepare whitepapers identifying models. Provide proposed statutory or regulatory language to the legislature or regulating body.
Educational	Importance of security parameters is not understood by all	Educate all users and governance groups.
Governance	Policy conflict in member organizations	Specify mechanisms to be used in conflict resolution as part of the legal agreements.

4. SUMMARY AND NEXT STEPS

Since health information technology will be a significant component in national plans to improve health care, the importance of privacy and security has become preeminent. However, the specifications to ensure standard application of best security practices across organizations have not been addressed. The Adoption of Standard Policies Collaborative (ASPC) has begun this work. This Guide to the Adoption of the Uniform Security Policy provides a framework designed to assist groups as they seek consensus on privacy and security practices to support the electronic exchange of health information and clears the path for addressing more of the critically important concerns that lie ahead.

Specifically, model policies for interstate exchange of health information are offered for authentication and audit. The other two security domains, authorization and access, were outside of the scope of the work of the ASPC during this specific project. However, having prioritized authentication as one cornerstone of privacy and security, and audit as the foundation for accountability and trust, a few aspects of authorization and access bled into the discussion. The more complete standardization of policies for these areas is one that remains open for the work of other groups. 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 exchange organizations, 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.

The Adoption of Standard Policies Collaborative recommends the following:

1. Testing the framework in environments (for example, Virginia/Tennessee and Washington/Oregon) that implement and assess the viability of the standard policies for authentication and audit.
2. Documenting the types of use cases and transactions that will and do occur in health information exchanges, to provide paradigms for policy and practice development for authorization, access, disaster recovery, archiving, and other intersecting domains.
3. Establishing or designating a rigorous and transparent policy review process, using the standards development, organizations, methodologies, and practices.
4. Standardizing the testing of the technology supporting these policies for the vendor market.

5. Evaluating the capacity to adhere to and support these policies as demonstrated in the certification of health information exchanges.
6. Providing funding for prototypes to test policy standards as they are technologically implemented.

In summary, the focus of health information exchange is the secure transmission of meaningful health data across organizational boundaries. The legal and policy context of health information exchange is found in federal rules and law that is further modified by state laws. The technical foundations for secure and private transport of health information are principles used to control the following:

- **Authorization** (who gets to view and edit the data)
- **Authentication** (how we know them to be who they assert)
- **Access** (what data they can access)
- **Audit** (the record of who has seen and changed what data)

The application of the principles outlined by these "4 A's" 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.

APPENDIX A:
FEASIBILITY: PREPARING FOR CHANGE AND PROCESS CHECKLIST

If your organization is interested in assessing the feasibility of adopting the Uniform Security Policy, it must first be prepared for the significant changes that will be required to adopt and implement these standards. The steps that follow in the change process are articulated in the checklist that follows in Section 2.

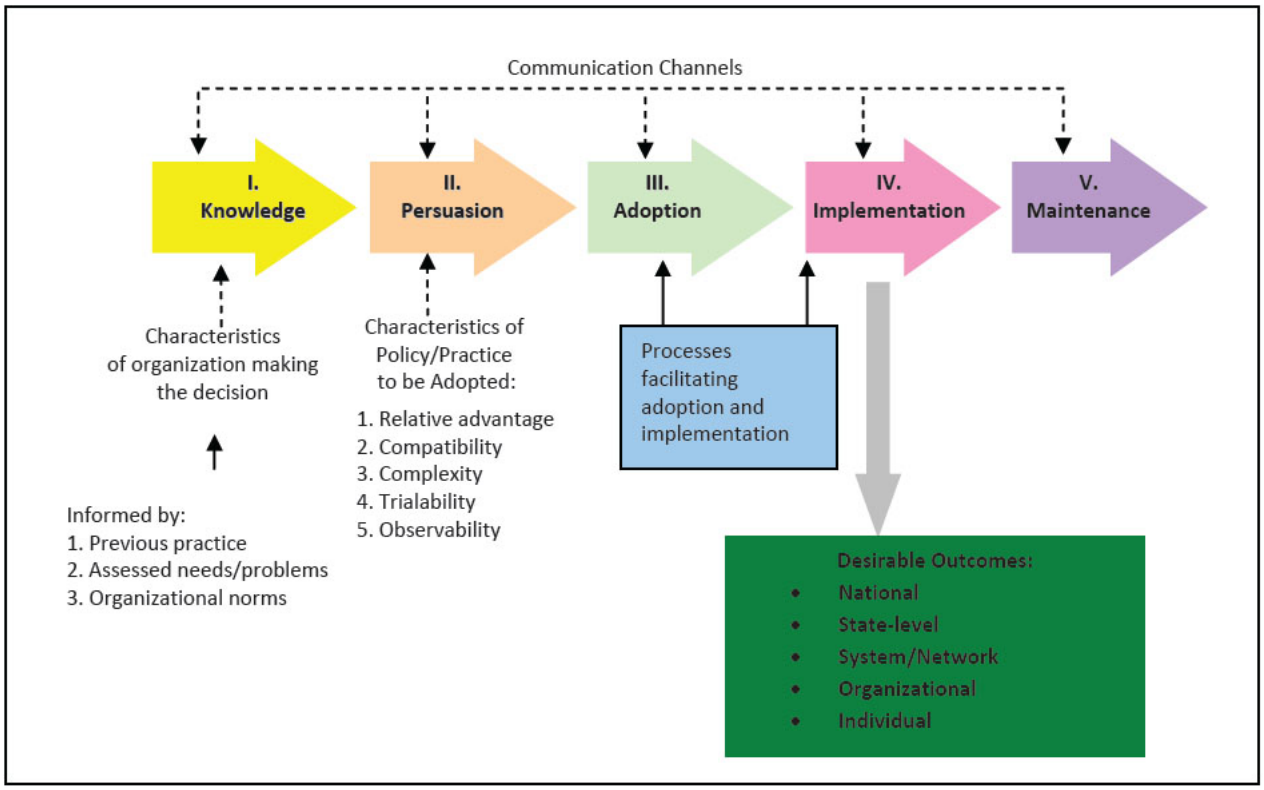
Section 1: Preparing for Change

To provide background for adopting the Uniform Security Policy, it is critical to understand the nature and context of organizational change, because change is a prerequisite to adoption. The organizational change perspective focuses on contextual features that enable an organization to respond to both internal pressures and external influences. The ASPC adapted its framework from Rogers' work on diffusion of innovative practices.[10] The diffusion model emphasizes characteristics of the policy/practice that may increase the likelihood of adoption by individuals and organizations. These complementary perspectives provide the framework that informed the recommendations for the adoption process proposed by the ASP Collaborative.

It is important to remember that any organizational change needs to involve senior organizational leadership for both public and private sector organizations. There needs to be a demonstrated value that can be bought in before senior leadership will consider adoption of the Uniform Security Policy, especially when that policy stretches beyond the bounds of an individual organization.

[10] Rogers, E. (2003). *Diffusion of innovations*. New York: Free Press.

Figure A-1. Diffusion of Innovations Model[11]



To use this framework to prepare for change, consider the following:

1. Is your organization prepared to ensure ***communication*** among organizational members as the central focus of all steps in the change process?
   - Transparent
   - Across many organization levels
   - Develop respect for the input of all
   - Organizational structure is important in facilitating the communication
2. Does your organization have the ***knowledge*** that it needs to implement minimum security standards for health information exchange?
   - Assess current policies, procedures, and practices
     - Internal
     - Industry specific
   - Needs assessment or gap analysis
   - Factors that impact change
     - Organizational culture
     - Professional norms

[11] Rogers, E. (2003). *Diffusion of innovations*. New York: Free Press, p. 170.

3. Is your organizational leadership ***persuaded*** to pursue this change to implement minimum security standards for health information exchange?
   - Relative advantage
     - Cost perception vs. value
   - Compatibility
     - Ease of transition
   - Complexity
     - Number of business units affected
   - Trialability
     - Proof of concept: Can we test the proposed innovation?
   - Observeability
     - Does system output reflect all processes?
     - Transparent functionality
4. Is your organizational leadership ***adopting*** minimum security standards for health information exchange?
   - Accept the proposed idea or innovation as a valued institutional goal
   - Awareness of the changes that will be required to adopt
   - Determined to proceed
   - Prepared to develop a change management plan and strategy, including the following:
     - soliciting feedback,
     - assessing adopter involvement or user attitude,
     - committing to the organizational investment (such as training and resources),
     - committing to the timeliness of delivery, ease of use,
     - evaluating the perceived efficiency and relevance of the policies and practices,
     - channeling information to organizational members,
     - conveying the salience of the practice,
     - actively enabling a change in behavior, and
     - documenting the change process.
5. Is your organizational leadership prepared to ***implement*** minimum security standards for health information exchange?
   - Require a focus of both management commitment of resources and research efforts
     - Aware of the types of change taking place within the organization
     - Internal barriers and facilitators
   - Require systemwide alterations and major changes at all levels of the organization
     - Requirements of resources
     - Centrality of consensus
   - Been adopted and accepted throughout the organization as standard practice

- Systematic and continuous evaluation
- Monitor outcomes

– Recording and communicating the progress of the change process

Section 2: Checklist

The following checklist is offered as a summary of steps described in the adoption guide. The purpose is to assist organizations in tracking progress of their adoption of the Uniform Security Policy. It may also be useful in assigning tasks and functions to actors in the HIO.

Summary of Steps: Goal and Scope

Goal and Scope	Check	Notes
Consider Pre-existing Structure	☐	—
Determine if this is an existing health information organization (HIO) or if an HIO is being planned	☐	—
If the HI0 exists, what level is it organized at:	☐	—
Local	☐	—
Substate region	☐	—
Substate region that crosses state lines	☐	—
State	☐	—
Multistate	☐	—
What are the existing agreements?	☐	—
Do these agreements include references to standards for:	☐	—
Authentication	☐	—
System to NHIN	☐	—
System to system	☐	—
Entity or individual to system	☐	—
Individual to participating entity	☐	—
Authorization	☐	—
License or credential checking	☐	—
Use of digital certificates	☐	—
System certification	☐	—
Automatic checks for changes	☐	—
Access	☐	—
Role definition:	☐	—
What are roles	☐	—
What roles see what data	☐	—
Web, intranet, or closed network	☐	—
Data use	☐	—
Use for treatment	☐	—
Use for medical analysis and consultation on behalf of a patient	☐	—
Secondary use of data	☐	—
Research	☐	—
Public Health	☐	—
Other (define)	☐	—

(continued)

Summary of Steps: Goal and Scope (continued)

Goal and Scope	Check	Notes
Audit	☐	—
Log generation (for example, network level, application level, transaction level, etc.)	☐	—
Log content specification	☐	—
Sharing logs/log reporting	☐	—
Failed logins/logins at inappropriate hours	☐	—
Audit policies and procedures (periodic and compliance)	☐	—
Investigation/mitigation/action for inappropriate use and disclosure	☐	—
Capability to change audit criteria and what is tracked	☐	—
Establish a privacy, technical security, and administrative/business security work group[12]	☐	—
Membership	☐	—
Chief Information Officer (CIO) from the highest level of organization	☐	—
Network engineer	☐	—
Application engineer	☐	—
Legal/compliance	☐	—
Human resources	☐	—
Chief Security Officer (CSO)	☐	—
Chief Privacy Officer (CPO)	☐	—
Management (business side)	☐	—
User	☐	—
Administrative policy	☐	—
Legislator	☐	—
Government (executive branch)	☐	—
Public information officer/communications	☐	—
Liaisons from other organizations, government, etc.	☐	—
Goal and Scope Milestones	☐	—
• Document the business model of the Health Information Organization	☐	—
• Collect and analyze existing agreements	☐	—
• Establish privacy, technical security, and administrative/business security	☐	—

[12]Because of potential breaches, this group needs to include representation from the general technical side, the general business side, the security side (administrative, physical and technical), the compliance side, and the privacy side. (Compliance needs to be included because of potential state law issues, differing federal laws such as GLBA for health plans, etc.)

Summary of Steps: Planning: Resources, Use Case, Risk Analysis and Legal

Planning: Resources, Use Case, Risk Analysis and Legal	Check	Notes
Existing policy and legal requirements are identified	☐	—
Legal counsel of the Health Information Organization governing authorities	☐	—
HISPC phase 1 and 2 findings[13] (if available for your state)	☐	—
CMS, OCR, other federal agencies, state agencies/attorney generals' office(s)	☐	—
Consent or authorization requirements	☐	—
Enacting the standards policy	☐	—
Legislation needed	☐	—
Regulation needed	☐	—
Contractual terms needed	☐	—
Inter-organizational agreement or Memorandum of Understanding (MOU) needed	☐	—
Define the scope	☐	—
Structure of the HIO: Treatment (individual) health vs. secondary use of data (such as Public Health business case)	☐	—
Use case definition	☐	—
Resource availability (fiscal, workforce)	☐	—
Realistic timeline	☐	—
Budget parameters (development and implementation as well as ongoing)	☐	—
Planning Milestones:	☐	—
• Summary report on organizational, state, local, regional, legal, and institutional (hospital, pharmacy, public health, worker's compensation, prisons, behavioral health, etc.) policy environment	☐	—
• Written plan to authorize the standards policy	☐	—
• Written plan to implement policy for the HIE	☐	—

[13] See the RTI International website (http://www.rti.org/) for information that pertains to the states and territories that you are working with. Another helpful resource would be the ASPC's ***Final Report***.

Summary of Steps: Implementation: Consensus, Testing and Deployment

Implementation: Consensus, Testing and Deployment	Check	Notes
Establish the implementation team	☐	—
Technical personnel	☐	—
Business managers	☐	—
Governance group for the organization	☐	—
Representatives from the user community	☐	—
Determine type of exchange to be tested	☐	—
Data elements	☐	—
Data formats	☐	—
Nomenclature	☐	—
System requirements	☐	—
Authentication	☐	—
Authorization	☐	—
Access	☐	—
Audit	☐	—
Business requirements	☐	—
Risk analysis	☐	—
Legal analysis (state and federal, and other regulatory or accreditation requirements appropriate to your situation)	☐	—
Policies and procedures	☐	—
Training (management and end users)	☐	—
Processes	☐	—
Participation	☐	—
Administrative Safeguards (partial list)	☐	—
Authorization, Authentication, Access and Audit	☐	—
Disaster Recovery/Emergency Mode Operations Plan (DRP/EMOP)	☐	—
Physical Safeguards	☐	—
Facility security	☐	—
Facility contingency plan (see DRP)	☐	—
Data Backup and Recovery	☐	—
Media and portable device management and controls	☐	—
Remote access management and controls	☐	—
Data and media disposal and re-use	☐	—
Security and Privacy Enforcement	☐	—
Testing Plan	☐	—
Minimum requirements specified	☐	—
Testing team	☐	—
Timeline and resources	☐	—
Data, applications, and processes to be tested	☐	—

(continued)

Summary of Steps: Implementation: Consensus, Testing and Deployment (continued)

Implementation: Consensus, Testing and Deployment	**Check**	Notes
Testing	☐	—
Remediation and documentation of testing results	☐	—
Approval	☐	—
Identification of who has authority to validate test results	☐	—
Retesting	☐	—
Acceptable completion	☐	—
Identification of who has authority to validate test results	☐	—
Deployment to production	☐	—
Certification and accreditation	☐	—
Deployment to production	☐	—
Production rules and procedures	☐	—
Incidence response	☐	—
Implementation Milestones:	☐	—
• Documentation of testing and remediation	☐	—
• Documentation for C&A	☐	—
• Go live	☐	—

Summary of Steps: Evaluation: Production, Training and Deployment

Evaluation: Production, Training and Deployment	Check	Notes
Risk analysis	☐	—
Review of audit reports	☐	—
Audit of authorized users	☐	—
Review of system performance	☐	—
Security breaches	☐	—
Data quality review	☐	—
User access data reviewed	☐	—
Evaluation Milestones:	☐	—
• Report to the Governing group	☐	—
• Report to funding source(s)	☐	—
• Ongoing training	☐	—
• Feedback to standards setting groups on the viability of minimum requirements	☐	—
• Required mitigation and mitigation plan development	☐	—
• Required policy, training, audit criteria, etc. review and revision	☐	—
• Documentation, document retention, and document destruction	☐	—

APPENDIX B:
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[14] and facilitation/support with the other ASPC states,[15] 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

[14] Arizona, Connecticut, Colorado, Nebraska, Oklahoma, and Washington.
[15] 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.[16] Reference: M2: A Model Contract for Health Information Exchange and P2: Model Privacy Policies and Procedures for HIE.

[16] 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*[17]

> *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.[18] 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,
- Clinical information contact,
- Service Location, and
- Predecessor name and date of change.

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

[18] 45 C.F.R. § 164.312(a)(2)(i) (requiring assignment of a unique name or number for identifying and tracking user identity).

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[19] is required for role-based access and should include the context of the organization. If the health care functional role[20] or the structural roles[21] exists, they are also required. *DAT 1*

[19] As defined in the American Health Information Community (AHIC) Use Cases.
[20] The functional role is dynamic and is a function of the role in which you are acting.
[21] A structural role is persistent and can be mapped to professions that are recognized.

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.[22]

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*

[22] 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.[23] *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

[23] 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[24] 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,[25] 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)

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

[25] 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,[26] 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

[26] 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[27]

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.

[27] 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).

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[28]

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 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

[28] 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").

1.5 Audit Trail and Node Authentication (ATNA)

The Audit Trail and Node Authentication Integration Profile[29] 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[30]

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[31]; however, some states may have longer retention requirements. *POL 17*

Section 3 - Information Access

3.1 Audit Controls[32]

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*

---

[29] IHE: Integrating the Healthcare Enterprise.
[30] HIPAA Security Rule 45 CFR § 164.308 (a)(8) – Evaluation.
[31] 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.
[32] HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls.

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

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[33]

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

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

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[34] 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*

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

[34] For example, the consent policy of the State of Massachusetts.

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 C:
OTHER USEFUL RESOURCES

- American Health Information Community (AHIC)
- American Health Information Management Association (AHIMA)
- Connecting for Health
- eHealth Initiative (eHI)
- Healthcare Information Management Systems Society (HIMSS)
- Healthcare Information Technology Standards Panel (HITSP)
- Integrating the Healthcare Enterprise (IHE)
- North Carolina Healthcare Information and Communications Alliance, Inc (NCHICA)

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

The American Health Information Community (AHIC) was formed to help advance efforts to reach President Bush's call for most Americans to have electronic health records within 10 years. The Community is a federally chartered advisory committee and provides input and recommendations to HHS on how to make health records digital and interoperable, and ensure that the privacy and security of those records are protected in a smooth, market-led way.

AHIC has developed a set of use cases outlining events and actions for different types of access to the health information exchange. The use case documents are available for download at the AHIC website.

The following use cases were utilized in developing the ASC standard policies:

- Laboratory Reporting
- Medication Management

American Health Information Management Association (AHIMA)
http://www.ahima.org/certification/maintenance.asp

The American Health Information Management Association (AHIMA) is the premier association of health information management (HIM) professionals. AHIMA is committed to advancing the Health Information Management profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning.

The Foundation of Research and Education (FORE) of AHIMA under contract to ONC has developed many practice and policy guidance documents for state-level HIE initiatives in the

areas of governance, structure, operations, financing, and HIE polices. The documents, as well as a tool kit, are available on the AHIMA website.

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

Connecting for Health is a public-private collaborative with representatives from more than 100 organizations across the spectrum of health care stakeholders. Its purpose is to catalyze the widespread changes necessary to realize the full benefits of health information technology, while protecting patient privacy and the security of personal health information. Connecting for Health is continuing to tackle the key challenges to creating a networked health information environment that enables secure and private information sharing when and where it is needed to improve health and health care.

The Common Framework helps health information networks to share information among their members and nationwide while protecting privacy and allowing for autonomy and innovation. It consists of 17 mutually reinforcing technical documents and specifications, testing interfaces, code, privacy and security policies, and model contract language. The documents are available for download at the Connecting for Health website.

The following framework documents were used in the development of the ASC standard policies:

- M1 – Key Topics in a Model Contract for Health Information Exchange
- M2 – A Model Contract for Health Information Review
- P5 – Authentication of System Users
- P7 – Auditing Access To and Use of a Health Information Exchange

Healthcare Information Management Systems Society (HIMSS)
http://www.himss.org/ASP/index.asp

The Healthcare Information and Management Systems Society (HIMSS) 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.

HIMSS provides resources, relevant news, and a toolkit to keep its membership and the community informed about the ever-changing areas of RHIOs and HIEs. The resources are available on its website.

Health Information Technology Standards Panel (HITSP)

http://www.hitsp.org/

The Healthcare Information Technology Standards Panel (HITSP) was founded in October 6, 2005, when awarded a contract award from the Office of the National Coordinator for Health and Information Technology (ONC) offered to advance President Bush's vision for widespread adoption of interoperable health records (EHR) within 10 years. The contracted targeted the creation of process to harmonize standards, certify EHR applications, develop nationwide health information network prototypes, and recommend necessary changes to standardized diverse security and privacy policies.

The American National Standards Institute (ANSI), in cooperation with strategic partners HIMSS, Booz Allen Hamilton, and Advanced Technology Institute, was selected to administer the standards harmonization initiative. The resulting collaboration became HITSP.

The Panel's work is driven by a series of priorities (Use Cases) issued by the American Health Information Community (AHIC). HITSP produces recommendations and reports in Interoperability Specifications and related Constructs that guide the standard implementation of each use case. The constructs consist of Interoperability Specifications, Transaction Packages, Transactions and Components. The recommendations, constructs and reports as well as a more in-depth explanation of the harmonization process are available on the HITSP website.

The HITSP Specifications and documents applicable to the use cases of Lab Reporting and Medication Management were utilized by the ASPC to harmonize policies with the use cases.

Integrating the Healthcare Enterprise (IHE)

http://www.ihe.net/

IHE is an initiative by health care professionals and industry to improve the way 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. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. The IHE Technical Framework documents are available on the IHE website.

North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)

http://www.nchica.org/

The North Carolina Healthcare Information and Communication Alliance (NCHICA) is a nationally recognized nonprofit consortium that serves as an open, effective, and neutral

forum for health information technology initiatives that improve health and health care in North Carolina.

NCHICA's leadership in conducting demonstration projects, hosting educational sessions, and fostering collective efforts within North Carolina helps position the state as a vanguard of national health IT acceleration efforts. NCHICA has developed a *Toolkit for State-Level HIE* to assist other communities, regions, and states develop a nonprofit similar to theirs. The Toolkit is located on the NCHICA website, under the "Health IT" tab.

eHealth Initiative (eHI)
http://www.ehealthinitiative.org/

The eHealth Initiative and the Foundation for eHealth Initiative are independent, nonprofit affiliated organizations whose missions are the same: to drive improvement in the quality, safety, and efficiency of health care though information technology. eHI focuses on the following topics to support its mission:

- Monitoring, assessing, and reporting out changes in the policy environment
- Developing multi-stakeholder consensus
- Developing and disseminating tools and resources
- Providing "hands-on help"
- Launching learning laboratories
- Expanding its coalition

Information about the eHI Blueprint and the eHealth Initiative Toolkit are available on its website.

National Institute of Standards Technology (NIST) 800 series of publications
http://www.nist.gov/index.html

Founded in 1901, NIST is a nonregulatory federal 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.

Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
http://csrc.nist.gov/publications/PubsSPs.html

APPENDIX D:
GLOSSARY AND ABBREVIATIONS

The following glossary includes the definition of key terms found in this Adoption Guide. A common understanding and use of these terms is critical in the consensus and adoption process.

This glossary represents an excerpt of terms included in a broader Glossary developed by the HISPC Adoption of Standard Policies Collaborative (ASPC) for the purposes of developing the Uniform Standard Policy. The full ASPC glossary can be found in the ASPC Final Report.

List of Terms

Term	Definition	Source of Definition
4 A's	Authorization, Authentication, Access, and Audit	HIPAA
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]
AHIC	American Health Information Community	Emergency Responder Use Case
AHIMA	The American Health Information Management Association	N/A
AHRQ	The Agency for Healthcare Research and Quality	N/A
Alliance	The State Alliance for E-Health	N/A
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

Term	Definition	Source of Definition
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. 5. 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
Authorization	The granting of rights, which includes the granting of access based on access rights.	[ISO 7498-2:1989]
Availability	The property of being accessible and useable upon demand by an authorized entity.	[ISO 7498-2:1989]
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
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
CMS	Centers for Medicare & Medicaid Services, a federal agency within the Department of Health and Human Services.	Medication Management Use Case

Term	Definition	Source of Definition
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
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
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 which 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
Demographics	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
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]
DRP/EMOP	Disaster Recovery Plan/Emergency Mode Operation Plan	N/A
eHI	The eHealth Initiative	N/A
Electronic Authentication	The process of establishing confidence in user identities electronically presented to an information system.	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

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
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
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
Health Record Banking	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 Registry	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 Care 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]
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 Collaboration	N/A

Term	Definition	Source of Definition
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
IHE	Integrating the Healthcare Enterprise 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
Integrity	Proof that the message content has not been altered, deliberately or accidentally, in any way during transmission.	Adapted from ISO 7498-2:1989
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 external nutrient solutions, oxygen, and other medical gases.	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

Term	Definition	Source of Definition
Minimum Policy Requirements	An agreed upon consensus set. They refer specifically to the policy requirements that the ASPC developed through extensive individual state review of current policy and the subsequent comparison and negotiation of these requirements across the 10 states in the collaborative. These minimum policies requirements become the framework across which the Uniform Security Policy was built.	Adoption of Standard Policies Collaborative
NCHICA	The North Carolina Health Information and Communications Alliance	N/A
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
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 nonregulatory 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
Node Authentication	Node Authentication - Describes authenticating each computer system in a network that can host one or more databases. [Each node in a distributed database system can act as a client, a server, or both, depending on the situation.]	Oracle
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
Organization Roles	Organizational roles correspond to the hierarchical organization in a company in terms of internal structures.	Neumann/ Strembeck

Term	Definition	Source of Definition
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/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
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]
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
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
Role	A set of competences and/or performances that are associated with a task	[ISO TS21298]
RTI	RTI International	N/A
Security	Combination of availability, confidentiality, integrity, and accountability.	[ENV 13608-1]
SLHIE	The State Level Health Information Exchange	N/A
Shared Secret	A secret used in authentication that is known to the Claimant and the Verifier.	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
Subscriber	A party who receives a credential or token from a CSP.	NIST 800-63-1

Term	Definition	Source of Definition
Token	Something that the Claimant possesses and controls (typically a key or password) used to authenticate the Claimant's identity.	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
Uniform Security Policy	Aggregated set of policies that the ASPC recommends organizations adopt as minimum policy to allow for interoperability with other organizations for health information exchange.	Adoption of Standard Policies Collaborative
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

APPENDIX E:
REFERENCES

AHIMA Home - American Health Information Management Association. (n.d.). Retrieved February 2009, from http://www.ahima.org

Connecting for Health. (n.d.). Retrieved February 26, 2009, from http://www.connectingforhealth.org

eHealth Initiative. (n.d.). Retrieved February 2009, from http://www.ehealthinitiative.org

HIMSS - RHIO. (n.d.). Retrieved February 2009, from http://www.himss.org/asp/topics_rhio.asp

HIMSS - RHIO. (n.d.). Retrieved February 2009, from http://www.himss.org/asp/topics_rhio.asp

Health Information Technology. (n.d.). Retrieved February 2009, from http://hhs.gov/healthit/ahic

Health Information Technology. (n.d.). Retrieved February 2009, from http://www.hhs.gov/healthit/privacy/statelevel.html

Healthcare Information Technology Standards - HITSP. (n.d.). Retrieved February 2009, from http://www.hitsp.org

IHE.net Home. (n.d.). Retrieved February 2009, from http://www.ihe.net

NCHICA Homepage. (n.d.). Retrieved February 2009, from http://www.nchica.org

National Institute of Standards and Technology. (n.d.). Retrieved February 2009, from http://www.nist.gov

National eHealth Collaborative (NeHC). (n.d.). Retrieved February 2009, from http://www.nationalehealth.org/

Rogers, E., & Rogers, E. M. (2003). *Diffusion of Innovations, 5th Edition*. New York City: Free Press.

The Privacy Rule. (n.d.). Retrieved February 2009, from http://hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

Welcome to NAHIT. (n.d.). Retrieved February 2009, from http://www.nahit.org

APPENDIX F: 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