PUBLIC HEALTH DATA STANDARDS CONSORTIUM

PHDSC

Promoting Standards Through Partnerships

**Privacy, Security and
Data Exchange (PSDE) Committee**

Analysis of Solutions and Implementation Plans Proposed by States to Address Privacy and Security Issues Affecting the Interoperability of Public Health Information Exchanges

A Review of State Findings from the Health Information Security and Privacy Collaboration Project

Project Report (2 of 2)

September, 2008

Table of Contents

b. State-level Implementation Plans

      i. Leadership and Governance
     ii. Practice and Policy
    iii. Legal and Regulatory
    iv. Technical and Standards
     v. Education and Outreach

5. Summary of Multi-State and National level Solutions and Implementation Plans Proposed by States to Address Variations in Public Health Related Privacy and Security Business Practices, Policies and State Laws

a. Analysis of Top Multi-State and National Solutions

6. Concluding Themes and Possible Roles, Opportunities and Areas of Work for the Consortium

1. Introduction

Background

From June 2006, to December 2007, 33 States and Puerto Rico participated in the first phase of the Privacy and Security Solutions for Interoperable Health Information Exchange project, a collaborative initiative funded by the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology (ONC) and managed by RTI International. Together, the State teams formed the Health Information Security and Privacy Collaborative (HISPC) and worked to reduce variation within each State and across the collaborative, identifying "good" practices that will permit interoperability while preserving privacy and security. [1]

During this period (HISPC Phase I), each State team followed a consistent and comprehensive process to:

1) Identify, document and analyze variations in organization-level business practices, policies, and State laws that affect electronic health information exchange;
2) Develop consensus-based solutions to reduce variations and other barriers to interoperability; and
3) Develop detailed plans for implementing solutions.

As a result of these intensive state-level deliberations and inter-state and national discussions, HISPC has collected a wealth of state-specific information on variations, proposed solutions and implementation plans to reduce or eliminate barriers to health information exchanges. The scenarios and areas covered by each state during HISPC Phase I included health care delivery (treatment), payment, operations, research, marketing and fundraising, Regional Health Information Exchange (RHIO)-related activities, and Public Health.

National reports summarizing the HISPC state-level findings have been produced and published by RTI. While these reports have provided a detailed picture of where states and the nation stand with respect to privacy and security issues across multiple domains, a more in-depth analysis of the

---

[1] Health Information Security and Privacy Collaboration (HISPC) – "Privacy and Security Solutions for Interoperable Health Information Exchanges" - http://healthit.ahrq.org/privacyandsecurity.

data collected on specific areas, such as public health, has not yet been completed (Fig. 1).

Building upon the work done by states during HISPC Phase I, the Public Health Data Standards Consortium embarked on a project to identify, extract, document and analyze all privacy-related variations, solutions and implementation plans reported by states and that directly affect Public Health.

Fig. 1
Horizontal and Vertical HISPC Scenario Analysis:
National HISPC Project and PHDSC Project Domain Depths

HISPC Scenarios						
	Treatment	Payment	Operations	RHIO	Public Health	....
National						
State 1						
State 2						
State 3						
...						

Current National-level Reports:
Aggregate Analysis of All State-All Scenarios (Horizontal Depth)

Consortium Project:
In-Depth Analysis of Public Health Scenarios (Vertical Depth)
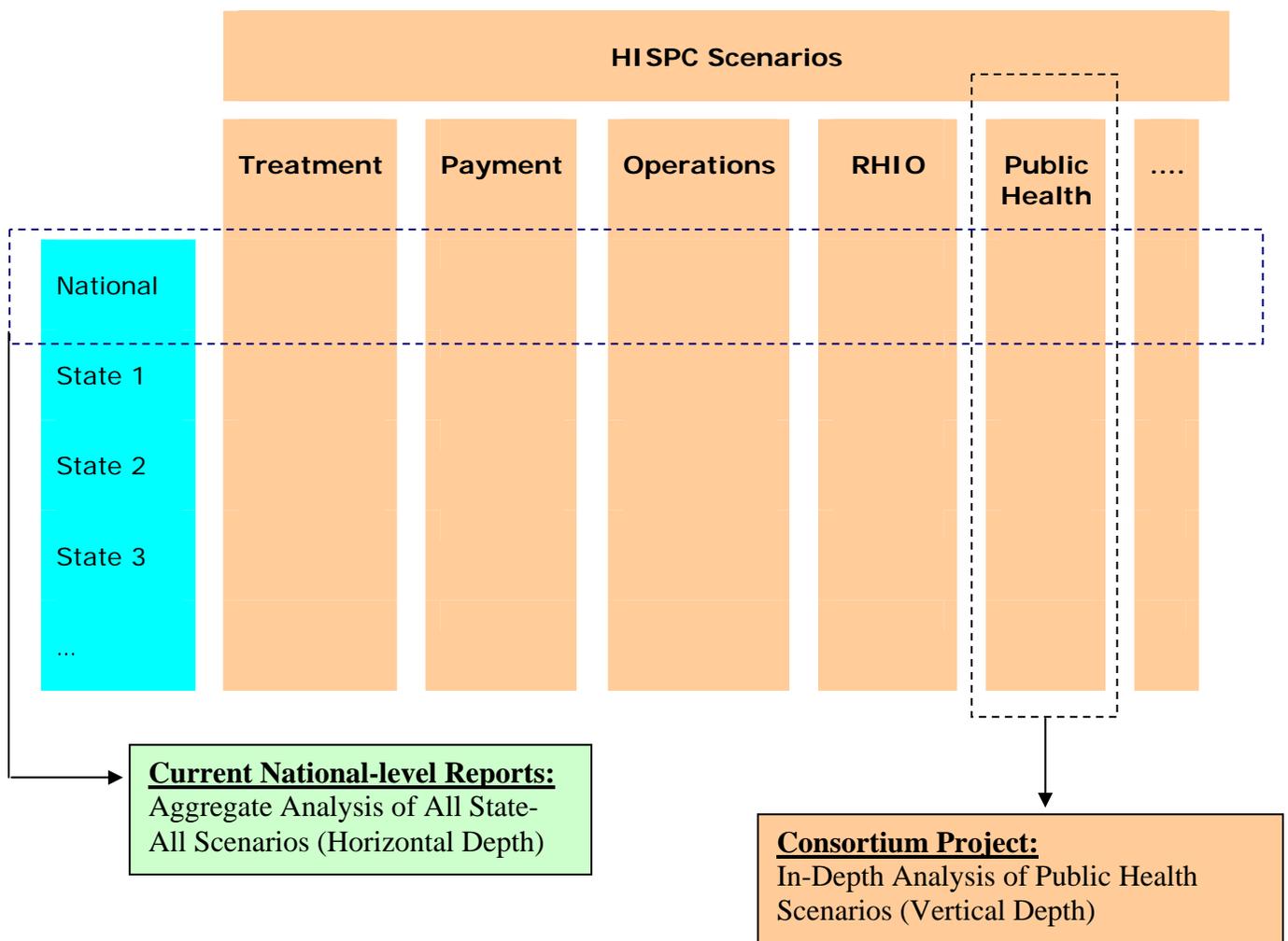
Purpose

The purpose of this project was to conduct a systematic, in-depth analysis of the Public Health Scenarios covered by all states during the HISPC Phase I project, building upon the detailed documentation of issues, variations, barriers, solutions and implementation plans, to identify best practice and guidance recommendations on how to address those issues that can be applied across states. Multi-state and national issues were also addressed.

The project was implemented under the direction of the Consortium's Privacy, Security and Data Exchange (PSDE) Committee. Funding was provided by the National Center for Health Statistics, Centers for Disease Control and Prevention, U.S. Department of Health and Human Services.

Project Report

This report summarizes the **solutions and implementation plans** identified by states to address barriers to health information exchanges caused by variations in privacy and security business policies, practices and state laws. A separate, first report on this project that focuses on the assessment of variations conducted by HISPC states is also available. Copies of these two reports are available from the Consortium website at http://www.phdsc.org.

The report first describes the methodology used by the Consortium in conducting this project, including research and collection of document sources, identification and extraction of public health-related information, analysis of findings and aggregation and reporting. Section 3 of the report provides a brief summary of the Consortium's **assessment of variations** report as a way of setting the stage. Section 4 presents the state-level solutions and implementation plans proposed by states. Section 5 summarizes the multi-state and national-level solutions and implementation plans proposed by states to address variations in public health related privacy and security business practices, policies and state laws. The report concludes with a summary of common themes and possible roles, opportunities and areas of work for the Consortium are highlighted.

The principal investigator for the project and lead author of this report was Dr. Walter G. Suarez, MD, MPH, President and CEO of the Institute for HIPAA/HIT Education and Research. The report was co-authored by Vicki Hohner, FOX Systems, and Co-Chair of the PSDE Committee.

2. Methodology

The methodological approach used by the Consortium to complete this project consisted of three core steps:

- Research and collect document sources
- Review, identify, select and extract information from document sources
- Aggregate and analyze extracted information

Research and Collect Document Sources

The first step in completing the project was to identify and collect key document sources from the HITSP Phase I project.   During HISPC Phase I, both states and the RTI team produced a number of documents, materials and resources including:

- At the state level:

    o Interim and final reports on the assessment of variations and analysis of solution
    o Interim and final reports on the implementation plans developed by states to address privacy and security barriers to health information exchanges

- At the national project level:

    o Interim Assessment of Variation of Business Practices, Policies and State Laws Report
    o Final Assessment of Variations and Analysis of Solutions Report
    o Final Implementation Plans Report
    o HISPC Toolkit
    o Nationwide Summary Report
    o Impact Analysis Report

Access to documents was achieved via the RTI and the AHRQ publicly-accessible project websites at http://www.rti.org/hispc and http://healthit.ahrq.gov/privacyandsecurity.

Identify, Select and Extract Public Health-Related Information

As stated earlier, the Consortium project focused on the Public Health scenarios used by HISPC states to assess variation, identify solutions and prepare implementation plans.

During the second part of the HISPC Phase I project, participating states identified a series of solutions to the issues and barriers documented in their Variations reports, and prepared a series of implementation plans for these solutions.

Aggregate and Analyze Extracted Information

All the information related to the solutions and implementation plans and that dealt directly with public health issues were systematically extracted and organized into a series of matrices for analysis.

State-level solutions and implementation plans were analyzed separately from multi-state/national level solutions and implementation plans.

Common solutions and implementation plans highlighted by a majority of states (as they were presented by the states in their reports) where identified, documented and analyzed for inclusion in this report, within the appropriate section. Issues that were noted by a small number of states were also highlighted. Multi-state and national issues identified by states were recorded.

Findings are summarized in Sections 4 and 5 of this report.

3. Summary of State, Multi-State and National-level Variations on Privacy and Security Business Practices, Policies and State Laws Affecting Public Health

The following two tables summarize the top state, multi-state and national-level issues identified by HISPC states that affect public health information exchanges, as documented and analyzed in the previous Consortium's report on this project. [2]

Table 1 State Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
Continued reliance on paper-based processes for public health information exchanges	■ There is continued reliance on paper-based processes when exchanging information with public health agencies. ■ Progress is being made on a number of public health programs, such as vital statistics, public health laboratory reporting and certain disease registries (i.e. immunization registries). ■ Still, other critical systems, such as biosurveillance and communicable disease reporting continue to operate mostly on paper.
Level of access by public health agencies to electronic health information during an emergency	■ Most access by public health agencies to health information during an emergency still occurs via phone, fax and paper methods. ■ Very little information, even when maintained electronically by the source, can be accessed by public health agencies. ■ This is mostly due to a lack of interoperability of electronic systems between public health agencies and providers (and other organizations) that maintain health information.

Table 1 State Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
Lack of business process/laws governing exchange of health information during bioterrorism events	■ States noted that there was a lack of routine business practices or specific state laws to guide or control access, use and disclosure of health information specifically during bioterrorism events.
Variations within a state on policies and procedures associated with the collection and reporting of communicable diseases and notifiable conditions	■ In some states, the issue continues to be the degree to which policies and practices vary on which conditions needs to be reported, what data to report, and what organizations must report, within the state. ■ This seems to be due greatly on a lack of understanding among reporting entities of the state public health laws.
Variability on the definition, reporting requirements and protections of 'sensitive' health information	■ There is significant variability on, or lack of, standard <u>definition</u>, <u>reporting requirements</u> and <u>protections</u> for 'sensitive' health information ■ Generally, 'sensitive' health information is understood to encompass general communicable diseases, more 'sensitive' communicable conditions (such as AIDS, STD), mental health, alcohol and substance abuse, reproductive health, and other information exchanged with public health agencies.
Exchange of data with public health agency under the HIPAA 'required by law' provision when a broad or no clear statutory requirement exists	■ Several states reported confusion among providers and other data submitters as to the degree of specificity of the statutory requirement to collect information that they maintain. ■ In some states, the statutory requirement is too broad and does not specify the data elements, type of information or sources of information from which the data is to be collected.
Voluntary vs. Authorized vs. Mandated exchanges of health information with public health agency for public health-related purposes	■ A number of states agreed there continues to be confusion regarding *when* certain health information exchanges must be statutorily <u>required</u> (as opposed to 'authorized' or be done in a 'voluntary' manner) and the degree of specificity needed on such statutory requirement (including definition of data elements to be reported, entities required to report, etc), and how data collection projects implemented by public health agencies with providers on a voluntary basis fit into these provisions.

Table 1 State Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
Exchange of data with health oversight agencies, including public health agencies, when only a broad statutory authorization exists	■ Several states reported that providers (and others) responsible for submitting health oversight-related information look for, or expect to be provided with a clear, unambiguous and detailed statutory requirement for reporting, rather than a broad, unspecific agency authorization to collect such information.
Variability of re-disclosure policies and practices between state and local public health agencies and across states	■ The lack of clear and unambiguous re-disclosure policies create significant concerns among providers responsible for submitting and disclosing health information to state and local public health agencies. ■ Stakeholders in most HISPC states expressed concerns with the fact that a HIPAA covered entity will have no control over the privacy and security of patient information once the information is released to a non-covered public health entity.
Administrative Issues Associated with Public Health Information Exchanges	■ Three sources of variation and general confusion related to the exchange of health information with state and local Public Health agencies commonly cited by HISPC states were: ■ The applicability of minimum necessary requirements to public health exchanges ■ The applicability of accounting of disclosure to public health exchanges ■ The confusion regarding whether to establish a business associate agreement with public health agencies to allow reporting of individually identifiable health information
Variability in the selection, implementation and use of core information security components of public health information exchanges	■ States identified the existence of significant variability on security standards and protocols used by different public health agencies (state, local within a state and across states) to identify and authenticate data users, authorize access to information, control access and perform audits on the access, use and disclosure of information.

Table 2 Multi-State and National-Level Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
Variation across states on collection and reporting of communicable diseases and notifiable conditions	■ Most states noted differences across states with respect to the collection of communicable diseases and notifiable conditions on at least four areas: ■ What conditions are to be reported; ■ How a condition is defined, a case is determined; ■ What data are to be reported; and ■ The reporting methods (paper, media, formats)
Variability across states on the definition, reporting requirements and protections of 'sensitive' health information	■ States identified a clear lack of definition of what constitutes 'sensitive' health information. ■ They also pointed out that differences between states on the definitions, reporting requirements and security protections to be used when collecting, maintaining, using and disclosing 'sensitive' health information create significant barriers to the implementation of public health information exchanges.
Exchange of public health data between states	■ Most states identified the lack of consistent methods and approaches to allow the exchange of different types of public health information between states as an important issue to be addressed. ■ From communicable disease data to registry data (such as immunizations) to more sensitive data (such as HIV/AIDS and mental health/chemical dependency data), most states implement such exchanges using a case-by-case approach, creating a multiplicity of customized, single-purpose agreements between states, between state and local public health agencies, and with tribes/Native American health services. ■ The need to establish standard inter-state agreements, state compacts or other forms of legal agreements to share individually identifiable health information during public health emergencies, and at other times, was noted.
Administrative Issues Associated with Public Health Information Exchanges	■ The three administrative-related issues associated with public health information exchanges described in the previous section (applicability of minimum necessary requirements to the public health exchange; applicability of accounting of disclosure to the public health exchanges; and the confusion regarding a need to establish a business associate agreement with public health agencies) were also highlighted as national-level issues.

Table 2 Multi-State and National-Level Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
Lack of consistent understanding and guidance on the interaction between federal and state laws affecting public health information exchanges	■ States frequently cited a persistent lack of consistent understanding and guidance availability on the interactions between federal and state laws affecting the exchange of health information with public health agencies, in areas such as alcohol and substance abuse, mental health, school records, and others.
FERPA limitations to allow sharing of school health records with outside entities, including public health agencies	■ FERPA imposes restrictions on the ability to share school health records, and specifically immunization data, with entities outside of the school, including public health agencies. This has continued to limit immunization registries' abilities to validate and provide complete and unambiguous immunization records of patients to providers at the point of care.
Lack of a public health privacy framework that would apply to public health participation in RHIOs and local, state, regional and national health information exchanges	■ As the country continues to see a progressive increase in the design, testing and implementation of local, state and regional electronic health information exchanges (HIEs), the roles, benefits and expectations of public health participation in such exchanges will continue to evolve. ■ One area of concern identified by states is the lack of a public health privacy framework for participation in such HIEs. Particularly with an increase in bi-directional communications between public health and public and private 'trading partners' expected, as well as increased access by public health to more clinical information for emerging public health activities such as syndromic surveillance and situational awareness.
Emerging issue: lack of a framework controlling the privacy of DNA and genetic-related health information	■ States reported increasing concerns regarding the lack of a national privacy framework that would protect the confidentiality of DNA and genetic-related health information and reduce or eliminate the risk of misuse of such information (i.e., for discrimination purposes). ■ Recently, Congress has passed, and President Bush has signed, the Genetic Information Nondiscrimination Act (GINA) which prohibits U.S. insurance companies and employers from discriminating on the basis of information derived from genetic tests. It forbids insurance companies from discriminating through reduced coverage or higher pricing and employers from making adverse employment decisions based on information derived from genetic tests. In addition, insurance companies and

Table 2 Multi-State and National-Level Issues Related to Variations in Privacy and Security Business Practices, Policies and State Laws	
Issue	**Brief Summary/Description of Issue**
	employers are not allowed to request or require a genetic test. ■ Still, there are some reported 'blind spots', particularly when it comes to privacy controls of genetic information. The new law does not seem to protect the genetic information collected by genetic testing companies which may use and even sell such information to outside parties.

4.   Summary of State-level Solutions and Implementation Plans

This section of the report presents the state-level solutions and state-level implementation plans aimed at addressing variations in privacy and security business policies, practices and state laws affecting public health information exchanges.

State-level solutions related to public health privacy and security issues can be organized into the following categories according to the needs they address:

- Public Health Reporting Policy
- Privacy Policy
- Security and Technical Standards
- RHIO/HIE-Enabling Policy
- Sensitive Health Information
- Education and Outreach
- Ancillary Issues (such as breaches and identity theft, genetic information, enforcement, and non-covered entities)

A. Public Health Reporting Policy

This was by far the area where most states offered recommended solutions. They included:

- Conduct a comprehensive review of state privacy and security laws and regulations affecting public health that are incomplete, fragmented or ambiguous and that were passed with a paper-based environment in mind and update, consolidate and simplify them.

- Review, and where necessary, revise definitions related to health information sharing and exchange that presently exist in statute to make them consistent for both a paper and electronic environment.

- Integrate state public health data systems into health information exchanges to 1) facilitate the monitoring of the health of communities, 2) assist in ongoing analysis of trends and detection of

emerging threats, and 3) provide information for setting public health policy.

■ Clarify, within a regional health information framework, how public health can participate, what information to or from public health can be shared, for what purposes, and what information public health can access and for what purposes.

■ Revise and modify, as necessary, reporting requirements and authorizations for data exchanges, such as communicable disease reporting, mental health records, immunization and other registry data.

■ Define and implement new regulations governing public and private information exchanges and authorities in the case of a bioterrorism event. Rules must be set up to clarify how and when information can be shared between private and public sector and with the Department of Health and Human Services and how and when information can be given to hospitals, practitioners and the public in the case of a bioterrorism emergency.

■ Establish general protocols for first responders and specify what information can be shared in given responding situations.

■ Clarify state statutes that establish exceptions to authorization requirements in the event of emergencies and for public health reporting purposes.

■ Modify state laws and regulations to facilitate the exchange of information for continuity of patient care purposes, including state agency participation. Many state agencies are restricted from exchanging patient specific data to other state agencies or providers of patient care. Modification of laws and/or regulations are needed to allow such agencies to establish "edge systems" and participate in appropriate health information exchange for care management, whereby they could still be the owners of the information that resides in their agency but also participate in HIE.

■ Work together to breakdown cultural and bureaucratic barriers and facilitate the sharing of data across programs by establishing practical administrative procedures for information sharing between state programs.

⇨ **In The Spotlight**

Colorado

Develop consensus regarding what public health information may be exchanged and if this should be subject to additional restrictions:

- Public health entities and programs must work with CORHIO to define levels of data sharing and enter into an agreement with CORHIO before public health data sharing is permitted.

- CORHIO will engage in a discussion to clarify which public health programs are willing to share public health data and for what purposes

- If public health data are to be shared, specific programs will need to become data sources and sign data sharing agreements with CORHIO.

- Public health programs will follow standard data sharing procedures and technical specifications for transmitting their data.

- Public health programs will need to determine whether audit features within CORHIO are sufficient or whether additional auditing measures will be undertaken within that program.

- At the time that a service is provided to a patient/client, public health programs that intend to share public health data will need to inform the patient/client of those practices.

- Clarifying the implications of current public health rules for information sharing related to medical treatment versus public health surveillance and intervention.

B. Privacy Policy

One of the most common areas states highlighted in their solutions and implementation plans was the need to develop, change, update, and integrate/consolidate their state privacy policies and laws, particularly those related to patient consent. In many cases, the public health agency will be the one responsible for bringing forward legislative initiatives to address these issues. The main areas covered included:

- Begin a process to update, consolidate and/or streamline the state statutes related to medical record confidentiality. Existing statutes are scattered throughout state laws and may or may not reflect HIPAA language or requirements. Consolidation and/or updates of statutes will help facilitate transition to electronic health information exchanges by clarifying rules for sharing health information.

- Special areas of interest to public health include: Medicaid regulations on privacy, additional state protections for 'sensitive' health information (such as HIV/AIDS, mental health, substance abuse, genetic information), sharing of information related to minors, and definition of a patient representative.

- Address the need for long term care providers to access health information about a patient and be able to deliver appropriate care, but it is unable to do so because the patient is physically or mentally unable to provide consent for the health information to be released to the long term care facility.

■ Create statutory definitions of several terms related to patient consent, including "health record", "identifying information", "Medical Emergency", "Related Health Care Entity", "Current Treatment", and "Record Locator Service".

■ Establish the statutory parameters for collecting, documenting and reporting patient consent electronically, including standards for accepting digital signatures.

■ Create a statutory framework for a provider to be able to rely on another provider's representation of having obtained patient consent to disclose health records.

⇨ **In The Spotlight**

__Indiana__

Indiana law provides for sharing of "health records" without patient consent for treatment purposes and legitimate business purposes (See Indiana Code 16-39-5-1). Health records include communicable disease information. There is, however, a statute in the public health law realm that appears, on its face, to require that "communicable disease" information may only be released for treatment purposes with the consent of the patient. To address this, Indiana proposed amending Indiana law (Indiana Code 16-41-8-1) to clarify that IC 16-41-8-1 does not apply generally to healthcare providers and that communicable disease data in providers' own medical records is governed by IC 16-39-1-1 et. seq

C. Security and Technical Standards

All states included in their solutions and implementation plans ways for public health agencies to begin addressing the core security, privacy and technical standards needed to ensure interoperable communications with external trading partners. These include:

- A major overarching privacy and security issue that must be solved to advance the automated, real-time electronic exchange of health information is to establish a framework and a common set of interoperable policies and technical requirements to address four core, interrelated security topics:

  - o Authorization
  - o Authentication
  - o Access Control
  - o Audit

- Public health agencies and their IT departments should conduct an assessment of their internal systems and identify areas where support for interoperable information exchanges will benefit the program, the agency and the community.

- Establish a body, in the form of an information technology security committee, to analyze, select, and recommend implementation strategies to establish standard security policies, procedures, and technology controls.

- Provide leadership to establish a standard business practice model, convene a statewide summit to share technology methodologies that address HIE privacy and security, and promote and ensure collaboration with other states and the federal government in the national HIT efforts and related activities.

- Adopt health information exchange standards to enable uniform anonymization and pseudonymization processes. Anticipating the need to support quality improvement, pay for performance and research initiatives, a uniform anonymization and pseudonymization approach is needed. The data would be assigned a re-linkable pseudo-identifier removing all other identifying data elements prior to submission of the data.

Of special interest were solutions to address the issue of <u>interoperable identification of users</u>:

- Provide for a reliable and secure method to correctly match patients with their health information, ensuring access to the right record(s) for the right patient at the point of care.

- Research and propose options on a system of patient identification that will allow speedy and convenient acquisition of information across jurisdictional lines when needed for interoperability.

- Establish a coordinated approach to identifying, authenticating and authorizing patients.

- One state government agency is considering assigning a unique health identifier to all residents in order to facilitate their identification across health information systems. Initially, the pilot project is considering implementing a unique health identifier by assigning a thirteen digit number to all potential participants in the public insurance plan, whether an application was approved or declined.

⇨ In The Spotlight

Rhode Island

- [AUTHENTICATION] Agree on policies and methods to identify persons and entities for purposes of controlling and monitoring access to the RI HIE and the protected health information that may be accessed through it; and for assuring the identity of persons (patients) that may authorize or restrict access to their individually identifiable health information through the RI HIE.

- [DATA PROTECTIONS] Agree on policies and methods to protect the privacy and confidentiality of health information (prevent unintended disclosure) and assure information integrity (detect unauthorized alteration) as it is transmitted to the RI HIE and as it is stored in the RI HIE.

- [RECORD MATCHING AND MERGING] Agree on policies and methods to enable the unique identity of patients and their corresponding health records to accomplish the correct matching of patient identifiers and merging of health records that originate from different sources into an integrated view of a specific patient's health information that can be accessed through the RI HIE by an authorized user.

- [AUDITING] Agree on policies and methods to log, track and report access to the RI HIE by any persons and entities, including the relevant details pertaining to all information disclosed through the RI HIE.

D. RHIO/HIE Enabling Policy

The design, planning, piloting and deployment of a RHIO and a state/regional HIE dominated solutions and implementation plans presented by states. Examples included:

- Introduce and adopt legislation to create the state's Health Information Network

- Provide financial support for RHIO activities through the joint pursuit of funding opportunities, including grants, fundraising, and government appropriations.

- Establish a Privacy and Security Committee of the state HIE and charge it with providing clarification on existing regulations and creating regulations that will advance HIE.

- Establish a state Health Information Technology and Exchange entity which will serve as a collaborative forum to promote HIT/HIE use and the adoption of a common HIT/HIE framework and principles.

- Develop and implement a pilot exchange project involving at least 3 distinct stakeholders in the local/state health care community (such as health center, hospital, lab, pharmacy, etc)

⇨ **In The Spotlight**

Connecticut

- Pursue legislation to authorize HIE Agent (RHIO) roles, accountability and functionality. Though the details of how to regulate the RHIO are still under discussion, some considerations in formulating the specifics behind this solution have been:
  - Connecticut state regulation of any RHIO to assure accountability of the RHIO and conformance with security and privacy considerations;
  - RHIO-Wide/Statewide Business Associate Agreements (BAA);
  - RHIO standard requirements;
  - Sanctions for violations of security/privacy or of RHIO policy;
  - Amend public health statutes;
  - Consider a digital signature law;
  - Update medical licensing laws; and,
  - Establish reporting requirements for metadata submission & minimal clinical data.

E. Sensitive Health Information

A common theme across states was addressing the variability in the use and implementation of the term 'sensitive' health information. Sensitive data is data often subject to greater standards of protection (needs some kind of definition here, even if just a list). Several solutions were offered on this issue:

- Recommend ways to reconcile differences between state and federal laws relating to the preemption and interpretation of sensitive health information.

- Develop a framework for RHIOs and HIEs to handle sensitive health information within a community and across states.

- Examine state laws that define 'sensitive'/'specially protected' health information to determine the appropriateness of the protections and the feasibility of implementing these protections in an electronic environment.

⇨ **In The Spotlight**

**Massachusetts**

The healthcare community must understand and address the need for improved management of sensitive information. The goal is to establish a clear understanding of what is sensitive medical information, so that we can develop a process across the stakeholder community which can support appropriate and trusted use of the information, including appropriate privacy and security controls.

The MA-HISPC Project will develop and disseminate a uniform definition, or set of definitions of the categories of sensitive clinical information based on state laws and regulations.

F. Education and Outreach

Health information exchange education and outreach was a fundamental component of all state solutions and implementation plans. Public health was specially referenced in many states as a source, a facilitator, the subject for, and the target of such initiatives. Examples included:

- Develop educational materials for consumers for providers to distribute.

- Establish core competencies for staff education.

- Mental health provider organizations and practice leaders should create an initiative and issue/publish statements and materials to educate all mental health providers that patient consent is not necessary for the disclosure of mental health records <u>for treatment purposes</u> (unless a state law requires it). The communication and education program should also include an explanation of psychotherapy notes to clarify any concerns in that regard.

- Promote the adoption of EMRs and best-in-class privacy and security practices in small and rural providers.

- Conduct joint training events for law enforcement and public health at annual conferences and seminars sponsored by local and state public health departments.

⇨ **In The Spotlight**

<u>*North Carolina*</u>

- Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.

- Develop programs to raise awareness on the risks, benefits, and impacts of health information technology to a cross-section of consumers.

G. Ancillary Issues

A host of solutions to a variety of state-level public health-related privacy and security issues were also identified by HISPC states, including:

<u>Uses of Health Data for Quality, Research, Public Health and Other Purposes</u>

- An examination of current practices for secondary use of data to determine an acceptable balance between ensuring that individually

identifiable health information is protected and making de-identified data available for appropriate use.

Breaches and Identity Theft

- An examination of state laws regarding breaches and identity theft to determine if they are appropriately and adequately addressed.

- Legislative or regulatory measures to address inappropriate disclosures and mitigate potential harmful effects of individually identifiable health information disclosure.

Genetic Information

- New legislation defining the privacy and security rules for genetic data. To promote consistency across state lines, it is further recommended that Oregon state regulatory guidance on the security of genetic data be used as model language.

- Establish well defined reporting requirements and confidentiality protections for rare genetic disorders, other disease registries and public health reporting requirements.

Enforcement

- Establish enforcement mechanisms to address privacy or security violations that occur among HIE participants.

Non-Covered Entities

- Establish legal privacy and security requirements for entities handling individually identifiable health information that are not covered by HIPAA.

5. Summary of Multi-State and National Level Solutions and Implementation Plans

A variety of multi-state and national-level solutions and implementation plans where offered by HISPC states. They included:

National Public Health Reporting Standards

- Create a plan to address the sharing of patient health information within states and across states in the event of natural or manmade disasters that result in patients being displaced.

Sensitive Health Information

- Address at the federal level the variations in definition, interpretation, protection and implementation of so-called 'sensitive' health information. Such information generally includes mental health, substance abuse, sexually transmitted diseases, reproductive health, genetic information, and others.

Inter-State Coordination and Agreements

- Establish national and regional multi-state task forces to develop standardized HIE policies and procedures for public health information exchanges between states.

- Develop standard inter-state agreements that support the exchange of public health and other health-related information.

- Set up state compacts to facilitate sharing of needed information across jurisdictions.

- Seek assurance that, to the extent possible, electronic health record information released to an out-of-state provider will receive the same level of protection that exists in the originating state.

HIPAA Regulatory Changes

■ <u>Business Associate Agreements (BAA)</u>: Remove the requirement to have a BAA, but instead hold business associates accountable for adhering to state and federal privacy requirements and liable for privacy violations under the law (i.e., extend the applicability of HIPAA to BAs).

■ <u>Minimum Necessary</u>: Remove the minimum necessary requirement and promote instead a "reasonableness" standard for release of health information.

■ <u>Accounting of Disclosures</u>: Remove or modify the requirements to document and account for public health-related disclosure purposes.

■ <u>De-identification; Limited Data Set; Designated Record Set</u>: Clarify the meaning and applicability of de-identification, limited data set, and designated record set to ensure consistent interpretation and usage.

■ <u>Non-Covered Entities</u>: Create legislative or regulatory measures pertaining to entities that handle individually identifiable health information and are not covered by HIPAA, requiring that, at a minimum, legal standards at a level equivalent to HIPAA be followed.

Changes in Other Federal Laws

Substance Abuse

■ Federal substance abuse regulations, Title 42 CFR, are very restrictive as they relate to the sharing of patient health information. Many states have developed state substance abuse laws, as well as mental health laws, that are comparable to federal substance abuse regulations. States are requesting that the federal substance abuse regulations found in Title 42 CFR be reexamined to assist with the goal of interoperability. Among the considerations, states point out to the following issues:

   o Address restrictions and limitations established by Federal Substance Abuse Treatment Information Regulations when reported to public health agencies. Specifically, amend 42 CFR

Part 2 to provide that patient consent is not required to exchange data for treatment purposes.

o Amend 42 CFR §§ 2.1 and 2.2, the Federal substance abuse treatment provisions, to allow for re-release of such information to health care providers <u>without</u> restrictions, for purposes of treatment.

o Clarify applicability of 42 CFR Part 2 in connection with the inclusion of patient information regarding alcohol and drug use in a HIE.

- Clarify that a comprehensive consent to participate in a HIE encompassing various categories of protected information, without a separate check-off for alcohol and drug abuse records, is acceptable. A national model form developed by the federal government will assist states and expedite the flow of information between states.

- Consider an exception in the 42 CFR Part 2 regulations so that when a person gives his/her consent to disclose their information "to a provider for treatment purposes," this allows disclosure of any and all information to a treating provider accessing the HIE — and not only access to a subset of the patient's information which might be determined to be necessary to treat the particular condition/illness.

Family Educational Rights and Privacy Act (FERPA)

- Amend FERPA to allow the release of student health records, particularly immunization information, to public health agencies and immunization registries.

- Review of FERPA restrictions on the authorized release of school health records in light of HIE Organizations that endeavor to support public health planning and disease surveillance activities.

Clinical Laboratory Improvement Amendments (CLIA)

- Amend 42 CFR §§ 493.1291(f) and 493.2 to solve CLIA issues, including restriction to report results only to the ordering provider.

- The intent of these amendments is solely to expand the list of permissible recipients of lab results, and <u>not</u> to expand the purposes for which those results may be disclosed. Therefore, these amendments would not permit a disclosure which the HIPAA Privacy regulations would otherwise prohibit (in the absence of state law restricting the list of permissible recipients of test results), and it would not permit the disclosure of a test result where state law prohibits disclosure of test results of that type due to their sensitive nature (*e.g.*, HIV results). Instead, the amendments would be aimed at scenarios in which the disclosure would be permitted by HIPAA but would be prohibited by state law merely because the intended recipient is not defined as an "authorized person" for receipt of lab results from a laboratory.

STARK

- The federal government should consider changes to Stark and anti-kick-back regulations that have resulted in barriers to the adoption of health information technology by providers.

Federal Programs and Agencies

- Require that all federal programs and departments conduct standardization efforts that complement and parallel individual states' efforts. The coordination of privacy and security standards for health information for the federal programs will facilitate nationwide implementation of HIE.

Addressing RHIO/HIE Status

- Address the legal status of RHIOs, including whether they should be considered Covered Entities, Business Associates or something else.

- Develop a framework for liability that addresses the role of the state level HIE organization/RHIO and the interaction of federal and state level regulatory frameworks.

- Develop model consent forms for loading information (routine and/or specially protected information) into a HIE.

- Develop model consent forms for disclosing Medicare information to and from a HIE (which could serve as a model to others).

- Monitor the development of opt-in/opt-out approaches for HIEs. Consider local, state and regional variations on such approaches and collect evidence on the health, economic, social, and other implications of each of these approaches. Continue to evaluate in an open, transparent, and public process, whether a national policy/framework on opt-in or opt-out is appropriate.

- Create a privacy and security certification process for HIE efforts.

National Coordination Bodies for Model Approaches and Legislation

- Work with the National Conference of Commissioners on Uniform State Laws (NCCUSL) to harmonize and develop model state laws addressing variations that hamper or limit public health information exchanges.

- NCCUSL could provide a forum for the discussion of specific areas of uniform consent and consent management, as well as sensitive clinical information.

Security and Technical Standards

- Develop national standard policies and practices for Authentication, Authorization, Access Controls and Audits.

- Utilize federal bridge to register, enroll, and integrate state based digital identity services.

- Promote the establishment of a national standard patient identification process/algorithm. Develop a pre-approved data set of patient identifiers to facilitate the correct pairing of patient records among different health information systems. Create an electronic process to track incidents in which the wrong patient record is matched.

- National standards defining security breaches exist (NIST, ISO, etc.) but could be clarified in terms of their relationship to electronic HIE.

Covered entities (including providers) are responsible under HIPAA to apply these standards, so education and clarification would be helpful regarding: what constitutes a security breach, notification requirements if information has been breached, and clear safe harbors for de-identified and encrypted information. National standards should override current state laws related to breaches and serve as a "ceiling" instead of a "floor".

- Require use of alternative mechanisms of authentication, such as biometrics, card swipes, USB keys, digital certification and other technology to improve the reliability of the authentication process.

- Promote the development of a state level mechanism, private or public, to manage the use of digital signatures in the health industry.

- Develop standards for the use of encryption to exchange patient health information.

Education and Outreach

- Create national standardized consumer education programs regarding secure and private use of individually identifiable health information. Educational efforts should be based on standardized marketing strategies that emphasize familiar cultural themes such as identity theft and social responsibility.

- Implement a public awareness campaign that will help the public understand what they stand to gain with increased exchange of health information and how their health information will be protected.

6.   Concluding Themes and Possible Roles, Opportunities and Areas of Work for the Consortium

Across the board, a comprehensive array of solutions and implementation plans were offered by states to address the variations on business policies, practices and state laws that affect public health information exchanges.

From a state-level perspective, Table 1 presents a summary of the overall category of solutions and implementation plans, a brief description of these solutions, and possible roles and opportunities for the Consortium.

Table 1
State-level categories of solutions and implementation plans and Possible Roles and Opportunities for the Consortium

Category	Summary of Solutions	Possible Consortium Roles and Opportunities
Public Health Reporting Policy	■ Conduct a comprehensive review of state privacy and security laws and regulations affecting public health. ■ Facilitate the integration of state public health data systems into health information exchanges ■ Develop a roadmap for how public health can participate on an HIE	■ Develop a template/tool for states to use when assessing the state privacy and security laws affecting public health ■ Facilitate the development of a roadmap for public health participation in HIEs
Privacy Policy	■ Develop, change, update, and integrate/consolidate state privacy policies and laws, particularly those related to patient consent. ■ Special areas of interest to public health include: Medicaid regulations on privacy, additional state protections for 'sensitive' health information (such as HIV/AIDS, mental health, substance abuse, genetic information), and sharing of information related to minors. ■ Establish the statutory parameters for collecting, documenting and reporting patient consent electronically, including standards for accepting digital signatures.	■ Research and document emerging state privacy policies, particularly those related to patient consent, opt-in/opt-out for HIEs, sensitive health information, and other topics.

Category	Summary of Solutions	Possible Consortium Roles and Opportunities
Security and Technical Standards	■ Establish a framework and a common set of interoperable policies and technical requirements to address Authorization, Authentication, Access Control and Audit. ■ Adopt health information exchange standards to enable a uniform anonymization and pseudonymization processes.	■ Facilitate the development of a security framework for public health on issues such as authentication, authorization, access control and audit ■ Help develop/promote a standard approach for anonymization and pseudonymization
RHIO/HIE-Enabling Policy	■ Introduce and adopt legislation to create a state Health Information Network ■ Establish a state Health Information Technology and Exchange entity which will serve as a collaborative forum to promote HIT/HIE use and the adoption of a common HIT/HIE framework and principles.	■ Monitor and document state legislation establishing/promoting local, regional and state HIEs and the participation of public health in them
Sensitive Health Information	■ Address the variability in the use and implementation of the term 'sensitive' health information.	■ Facilitate the development of a standardized approach to sensitive health information

Ancillary Issues	■ Address issues related to:
	  o Use of health information for Quality, Research, Public Health and Other Purposes
	  o Breaches and Identity Theft
	  o Privacy and security of genetic-related information
	  o Enforcement of privacy and security regulations
	  o Handling of non-covered entities
		■ Prioritize and facilitate and/or participate in working groups to address the various ancillary issues identified by states

Education and Outreach	■ Health information exchange education and outreach was a fundamental component of all state solutions and implementation plans. Public health was specially referenced in many states as a source, a facilitator, the subject for, and the target of such initiatives.	■ Be actively engaged in regional and national education and outreach efforts ■ Develop templates and tools to assist states with education and outreach efforts

From a national-level perspective, Table 2 summarizes the core categories of solutions and implementation plans, the general issues being addressed by the proposed solutions, and possible roles and opportunities for the Consortium.

Table 2
National-level categories of solutions and implementation plans and Possible Roles and Opportunities for the Consortium

Category	Summary of Solutions	Possible Consortium Roles and Opportunities
National Public Health Reporting Standards	■ Develop a framework for sharing individually identifiable health information across states in the event of emergencies, disasters and bioterrorism	■ Assist in coordinating the development of framework
Inter-state Coordination and Agreements	■ Establish national and regional multi-state task forces to develop standardized HIE policies and procedures for public health information exchanges between states. ■ Develop standard inter-state agreements that support the exchange of public health and other health-related information.	■ Facilitate the formation of such multi-state working groups ■ Work with other national initiatives to develop standard inter-state agreements

HIPAA Regulatory Changes	■ Address the following issues:
	  o Business Associate Agreement
	  o Minimum Necessary
	  o Accounting of Disclosure
	  o De-identification, Limited Data Sets, Designated Record Set
	  o Non-Covered Entities
		■ Prioritize and work on addressing the identified issues

Changes in Other Federal Laws	■ Address issues related to the following federal laws and regulations:
	  o Substance Abuse
	  o FERPA
	  o CLIA
	  o STARK
		■ Prioritize and work on addressing the identified issues

Sensitive Health Information	■ Address at the federal level the variations in definition, interpretation, protection and implementation of so-	■ Assist the federal government in developing a common

Category	Summary of Solutions	Possible Consortium Roles and Opportunities
	called 'sensitive' health information.	approach to sensitive health information.
Addressing RHIO/HIE Status	■ Address the legal status of RHIOs, including whether they should be considered Covered Entities, Business Associates or something else. ■ Develop a framework for liability that addresses the role of the state level HIE organization/RHIO and the interaction of federal and state level regulatory frameworks. ■ Develop model consent forms for loading information (routine and/or specially protected information) into a HIE.	■ Work with the federal government to address the legal status of RHIOs and other similar organizations involved in HIEs.
Security and Technical Standards	■ Develop national standard policies and practices for Authentication, Authorization, Access Controls and Audits. ■ Utilize federal bridge to register, enroll, and integrate state based digital identity services. ■ Promote the establishment of a national standard patient identification process/algorithm. ■ National standards defining security breaches exist (NIST, ISO, etc.) but could be clarified in terms of their relationship to <u>electronic</u> HIE.	■ Work with partners to develop national standard policies and practices on security issues such as authentication, authorization, access control and audit.
Education and Outreach	■ Create national standardized consumer education programs regarding secure and private use of individually identifiable health information. ■ Implement a public awareness campaign that will help the public understand what they stand to gain with increased exchange of health information and how their health information will be protected.	■ Work with ONC and others to coordinate a national consumer education campaign regarding secure and private use and disclosure of individually identifiable health information.