PUBLIC HEALTH DATA STANDARDS CONSORTIUM

PHDSC

Promoting Standards Through Partnerships

Privacy, Security and Data Exchange (PSDE) Committee

Assessment of Variations in Privacy and Security Policies, Practices and State Laws Affecting the Interoperability of Public Health Information Exchanges

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

Project Report (1 of 2)

September 2008

Table of Contents

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.

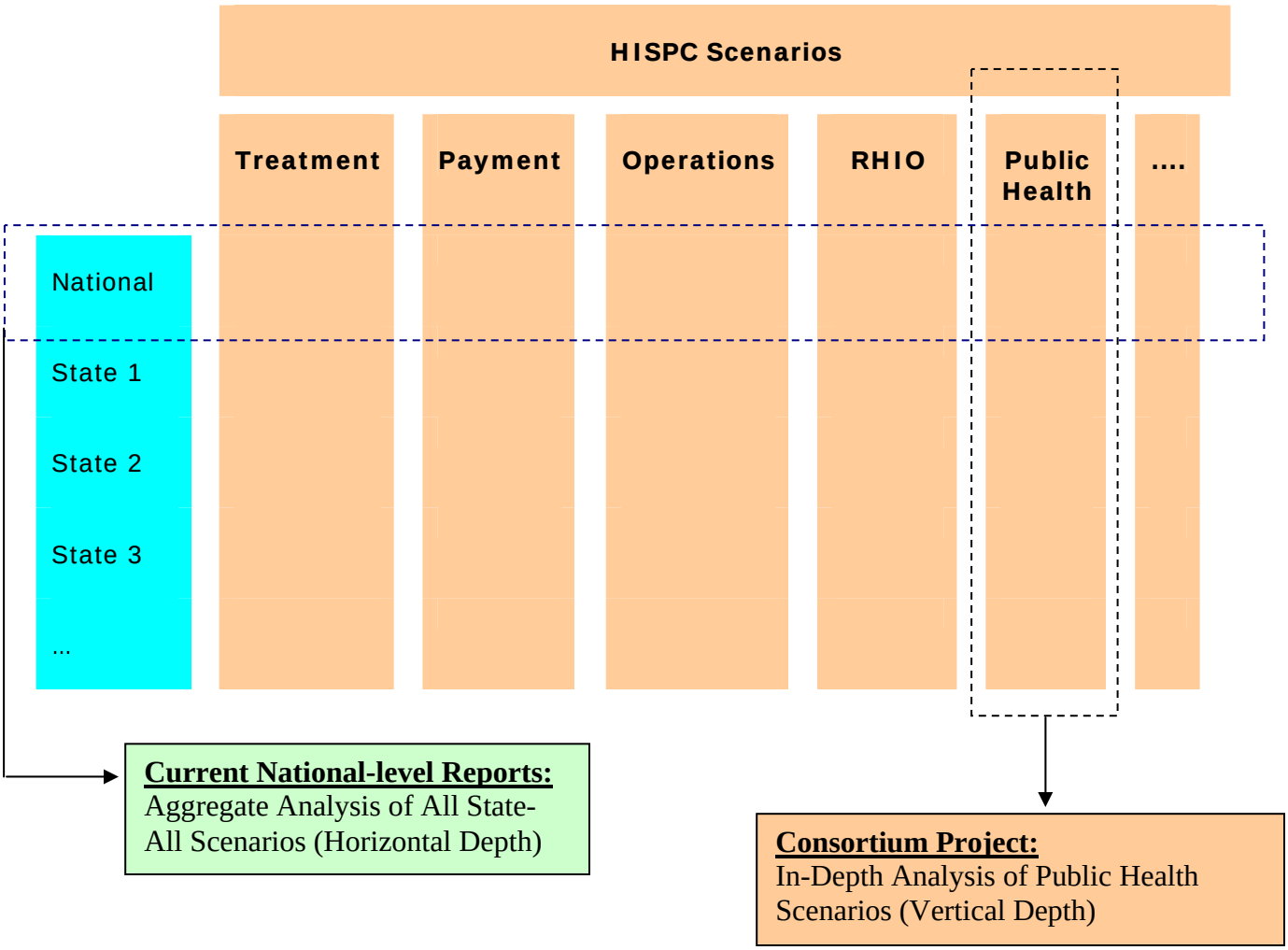
National reports summarizing the HISPC state-level findings have been produced and published by RTI. While these reports have provided a detailed picture of where states and the nation stand with respect to privacy and security issues across multiple domains, a more in-depth analysis of the

[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



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 **variations** in privacy and security policies, practices and state laws affecting the interoperability of public health information exchanges, as identified by states. A separate, second report on this project focuses on the analysis of solutions and implementation plans proposed by states and aimed at addressing barriers to public health information exchanges. 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. A review of the public health scenarios and privacy and security domains used by HISPC is then presented, followed by a summary and analysis of the top state-level issues identified by states and that relate to variations in public health-related privacy and security business practices, policies and state laws. A summary and analysis of the top multi-state and national public health-related privacy issues identified by states is then provided. 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:
    - Interim and final reports on the assessment of variations and analysis of solution
    - 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:
    - Interim Assessment of Variation of Business Practices, Policies and State Laws Report
    - Final Assessment of Variations and Analysis of Solutions Report
    - Final Implementation Plans Report
    - HISPC Toolkit
    - Nationwide Summary Report
    - 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.

HISPC participating states were provided with 18 hypothetical health information exchange scenarios to use as a means to elicit discussion among stakeholders and identify and document variations in policies, practices and state laws that affect health information exchanges. The scenarios provided a standardized context for discussing organization-level business practices across all states and territories.

The scenarios represented a wide range of purposes for the exchange of health information that take place within a broad array of organizations, including treatment, payment, operations, biosurveillance, health oversight, research, and marketing. Of the 18 scenarios, five dealt directly with public health issues, including 1) Bioterrorism Event; 2) Active Carrier, Communicable Disease Notification; 3) Newborn Screening; 4) Homeless Shelters; and 5) Health Oversight – Legal Compliance/Government Accountability.

A more detailed description of these scenarios is provided in Section 3.

All information related to the assessment of variations from these five scenarios included in the HISPC reports was systematically extracted and organized by scenario and state into a series of matrices for analysis. In addition, information relevant to public health that was included in other scenarios (i.e. research, operations, RHIO) was also extracted if it had a direct relationship to public health activities.

Aggregate and Analyze Extracted Information

A series of tables capturing variation issues by state were created to document and assist in the aggregation and analysis of data. Common themes and related issues highlighted by a majority of states were identified and analyzed. 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. HISPC Public Health Scenarios and Privacy and Security Domains

As noted above, HISPC participating states were provided with 18 hypothetical health information exchange scenarios to use as a means to elicit discussion among stakeholders and identify and document variations in policies, practices and state laws that affect health information exchanges. The scenarios represented a wide range of purposes for the exchange of health information (e.g., treatment, biosurveillance, payment, research, and marketing) that take place within a broad array of organizations. The scenarios were developed by the American Health Information Management Association (AHIMA) to provide a standardized context for discussing organization-level business practices across all states and territories.

In addition, 9 Privacy and Security Domains where provided to states (including such areas as authentication, authorization, access controls, transmission security, patient and provider identification) to use in the analysis of each of the scenarios, and to organize the identified variations in business policies, practices and state laws. The selected domains represent the core security and privacy concepts that more commonly affect interoperability and electronic health information exchanges, when variations on how they are implemented exist across and between organizations.

A. Description of Public Health Related Scenarios

Of the 18 scenarios, five dealt directly with public health issues, including:

- Bioterrorism Event
- Active Carrier, Communicable Disease Notification
- Newborn Screening
- Homeless Shelters
- Health Oversight – Legal Compliance/Government Accountability

Following is a brief description of these scenarios:

Scenario 13 – Bioterrorism Event

Stakeholder organizations and exchange roles:

- Laboratory (collecting data)

- Health care provider (transmitting data to public health)
- Public health department (receiving data from provider, providing data to government agencies)
- Law enforcement (receiving data)
- Government agencies (receiving data)
- Patients (providing data, receiving data)

Scenario Description:

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the state declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well as informing the regional media to alert the public to symptoms and seeking treatment if feeling affected. The state also notifies the federal government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as it arises to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Potential areas of discussion of **business practices** based on this scenario: 1. Providing patient-specific information related to specific symptoms to law enforcement, CDC, Homeland Security, and health department in a situation where a threat is being investigated.

Scenario 15 - Active Carrier, Communicable Disease Notification

Stakeholder organizations and exchange roles:

- Health care provider (sending initial data to public health and lab, receiving data on follow up)
- Public health department (receiving data, sending data)
- Law enforcement (receiving data)
- Patient (providing data, receiving data)

Scenario Description:

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multidrug resistant). The patient purchases a bus ticket—the bus ride will take a total of 9 hours with 2 rest stops across several states. State A is made aware of the patient's intent 2 hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Potential areas of discussion of **business practices** based on this scenario: 1. Providing patient-specific information related to a specific communicable disease to law enforcement, non–health care entities, and health department in a situation where a threat is being responded to. 2. Ensuring the data is secured as it is transmitted

Scenario 16 - Newborn Screening

Stakeholder organizations and exchange roles:

- Health care provider (sending initial data to public health and lab, receiving data on follow up/eligibility)
- State laboratory (receiving data)
- State public health department (receiving data, sending data)
- Parent (receiving data)

Scenario Description:

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Potential areas of discussion of **business practices** based on this scenario: 1. Providing patient-specific information related to specific symptoms of a disease to a health department in a situation where a targeted disease or condition is being investigated.

Scenario 17 - Homeless Shelters

Stakeholder organizations and exchange roles:

- Primary care provider (sending) and hospital-affiliated drug treatment center (receiving)
- The hospital-affiliated drug treatment clinic (releasing) and the county program (requesting for purposes of reimbursement)
- The hospital-affiliated drug treatment clinic (releasing) and the shelter (requesting to verify the treatment)
- The family member (requesting) and the shelter (sending)

Scenario Description:

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary care provider, and he is sent there for medical care. Primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

Potential areas of discussion of **business practices** based on this scenario: 1. The extent and amount of information shared between the various facilities would be limited by the minimum necessary and confidentiality guidelines.

Scenario 18 - Health Oversight: Legal Compliance/Government Accountability

Stakeholder organizations and exchange roles:

- State university faculty (requesting health information)
- State public health agencies (asked to provide health information)

Scenario Description:

The governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient-level health care data on an ongoing basis to determine if the children are getting the health care they need. This is not part of a legislative mandate. The governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is no existing contract with the state university for services of this nature.

Potential areas of discussion of **business practices** based on this scenario: 1. What is the practice of the organization to provide appropriate information for health care oversight activities? These may include: – Determining minimum amount necessary. – How to release (electronically or paper—with existing claims data). Include whether or not the information can or should be shared; under what conditions; and whether some form of contract or agreement is required.

B. Nine Domains of Privacy and Security

The nine domains provided to states to use in analyzing the 18 scenarios were:

1. **Authentication:** User and entity authentication to verify that a person or entity seeking access to electronic individually identifiable health information is who they claim to be.

2. **Authorization and Access Control:** Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic individually identifiable health information.

3. **Patient and Provider Identification:** Patient and provider identification to match identities across multiple information systems and locate electronic individually identifiable health information across enterprises.

4. **Transmission Security:** Information transmission security or exchange protocols (i.e., encryption) for information that is being exchanged over an electronic communications network.

5. **Information Protection:** Information protections so that electronic individually identifiable health information cannot be improperly modified.

6. **Information Audits:** Information audits that record and monitor the activity of health information systems.

7. **Administrative Security:** Administrative or physical security safeguards required to implement a comprehensive security platform for health information technology.

8. **State Law:** State law restrictions on certain information types and classes and the solutions by which electronic individually identifiable health information can be viewed and exchanged.

9. **Policy:** Information use and disclosure policies that arise as health care entities share individually identifiable health information electronically.

4. Summary of State-Level Issues

This section of the report provides a summary of the top issues identified by HISPC states that result from variations in privacy and security business practices, policies and states laws and that directly affect public health information.

Issue 1 – Significant continued reliance on paper-based processes for public health information exchanges

Almost all states reported as a common concern the 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) but other critical systems, such as biosurveillance and communicable disease reporting, are still operating mostly on paper.

Issue 2 – Level of access by public health agencies to electronic health information during an emergency

While there was general consensus across states that public health agencies have had good access to individually identifiable health information during outbreaks and natural disasters, most of the access still occurs via phone, fax and paper methods. Very little information, even when it is maintained electronically by providers, 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 individually identifiable health information.

Issue 3 – Lack of business process and laws governing the exchange of health information during bioterrorism events

While bioterrorism events are relatively rare in most states, there is a noted lack of routine business practices or state laws in place to guide or control access, use and disclosure of health information during such events.

Some states have a bioterrorism registry statutorily established, but there seems to be a lack of understanding among providers and others on the purpose and use of these registries.

Misunderstanding of, and variability in, the role and ability of law enforcement to intervene during a bioterrorism event, including the ability to access identifying information about an individual who may be carrying a disease, was also identified as an issue.

In many states, specific rules governing the handling and/or security of data during different bioterrorism events do not exist. Stakeholders are forced to use other rules (i.e., tuberculosis rules) as guidelines.

Issue 4 – Variations within a state on policies, practices and state laws associated with the collection and reporting of communicable diseases and notifiable conditions

There was general consensus and across-the-board understanding among states that when it comes to public health surveillance, communicable disease reporting supersedes all patient confidentiality laws, including HIPAA. If an individual contracts a disease that is a threat to public health (generally classified as a reportable/notifiable condition), patient information related to such condition must be disclosed by the provider to the appropriate public health agencies promptly, and this can be done without the patient's authorization or consent, or even over the confidentiality objections from the patient.

Communicable disease reporting happens constantly at various levels (federal, state, local) and for multiple conditions and reasons, and extensive policies, practices and state and federal laws exist related to who can access, use or disclose such individually identifiable health information, when, how, to whom and for what purpose.

Several states reported that they have clear guidance, processes and forms (defining the data elements and content to be reported) in place and that the issue was a lack of knowledge, understanding and the need to periodically re-train or inform those reporting.

In some states, the issue still is the degree to which these policies and practices vary across conditions and organizations within a state (less often an issue, although still reported by a number of states, mostly caused by a lack of understanding among reporting entities of state public health laws).

Issue 5 – Variability within a state on the definition, reporting requirements and protections of 'sensitive' health information

One of the most commonly cited variation issues related to the exchange of health information with public health agencies was the variability both within a state and across states on the definition, reporting requirements and protections that need to be afforded to 'sensitive' health information. The term has not been consistently defined, which was one of the main issues noted by states to be addressed in the future, but generally referred to individually identifiable health information that includes 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.

How one entity understands and operates internally (internal business practices and policies) with respect to such sensitive information differs from how another entity within a state does it. This is generally due to a lack of understanding (and sometimes lack of existence) of standardized policies, practices and state laws coming from the public health agency.

Issue 6 – Exchange of data with public health agency under the HIPAA 'required by law' provision when a broad or no clear statutory requirement exists

Under HIPAA, covered entities are permitted to disclose protected health information to appropriately authorized agencies, including public health agencies, to the extent that such disclosures is required by law and the disclosure is limited to the relevant requirements of such law.

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.

Issue 7 – Voluntary vs. Authorized vs. Mandated exchanges of health information with public health agency for public health-related purposes

Under HIPAA, covered entities are permitted to disclose protected health information to public health authorities that are authorized by law to collect or receive such information for the purposes of preventing or controlling

disease, injury or disability, including (but not limited to) the reporting of disease, injury and vital events such as birth or death, the conduct of public health surveillance, public health investigation and public health interventions, and the detection and management of child abuse or neglect cases.

A number of states agreed that there is some confusion regarding when such health exchanges are required; the degree of specificity needed on the statutory authorization to collect, use and disclose such information (including the data elements to be reported and the entities that must report); and how data collection efforts implemented by public health agencies on a voluntary basis fit into these provisions.

Issue 8 – Exchange of data with health oversight agencies, including public health agencies, for health oversight purposes when only a broad statutory authorization exists

Under HIPAA, covered entities are permitted to disclose protected health information to health oversight agencies for oversight activities that are authorized by law, such as audits, civil, administrative or criminal investigations, inspections, licensure or disciplinary actions and other activities for appropriate oversight of the health care system.

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.

Issue 9 – Variability of re-disclosure policies and practices between state and local public health agencies and across states

Another frequently cited issue was the variability of re-disclosure policies across state and local public health agencies and, in particular, across states.

In most cases, state laws regulate what, when, how, to whom and for what purposes public health agencies can disclose health information that they collect, maintain and use. In most states these laws are narrowly focused and specific to the type of information collected. Noticeable differences exist from state to local public health agencies, and between local public health agencies. These differences are only amplified when looking across states.

Still, the lack of clear and unambiguous re-disclosure policies and practices between state and local public health agencies and across states create significant concerns among providers that are responsible for disclosing health information to such agencies.

On a related issue, 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. Such a non-covered entity would have a separate and different set of privacy and security controls (sometimes more stringent, sometimes less stringent) than the ones imposed on covered entities.

Once the protected health information is released to a non-covered entity, the controls over potential uses and re-disclosures of such information by these non-covered entities were unclear and inconsistent, and the processes for handling the health information varied among different state and local public health agencies.

Issue 10 – 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: except when mandated by law (which requires that the collection be limited to the relevant requirements of such law), entities reporting to public health and health oversight agencies must rely on those agencies as to what is the minimum data they need for the purpose for which the data is being collected.

- The applicability of accounting of disclosure to public health exchanges: an issue that continues to cause much concern among those entities that must maintain an accounting of such disclosures.

- The confusion regarding whether to establish a business associate agreement with public health agencies to allow reporting of individually identifiable health information: public health agencies continue to have to clarify with data submitters that there is NO need to establish such

agreements when the collection is done for purposes required by law, public health functions or health oversight reasons.

Issue 11 – Variability in the selection, implementation and use of core information security components of public health information exchanges

One of the most critical security-related variation issues affecting health information exchanges highlighted by most states is the significant variability on 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.

There were frequent concerns expressed with regard to the inability of information systems to appropriately authenticate users' identities during emergency situations (such as natural disaster events), thus not protecting the privacy and security of health information. The technology exists to authenticate users, but it is not relied upon during these emergencies.

Inconsistency in the methods used by various entities to ensure that messages communicated by public health reached the right person (acknowledgement, audit controls) was also a commonly cited concern.

This inability to reliably determine that urgent communications have been delivered and received through electronic systems is seen as one of the primary barriers to the use of health information exchanges in a bioterrorism event.

States also reported significant variability and inconsistency in using secure data transmission methods (i.e. encryption, secure email, SSL, etc) when exchanging data electronically.

5. Summary of Multi-State and National Level Issues

This section of the report summarized the top multi-state and national-level privacy and security issues identified by HISPC states that directly affect public health information exchanges. Some of these issues have already been discussed in the previous section, as they also touch on state-level concerns.

Issue 1 – Variation across states on policies, practices and state laws associated with the 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 forms, media, formats, etc)

Issue 2 – Variability across states on the definition, reporting requirements and protections of 'sensitive' health information

The issues around lack of consistency within a state as to what constitutes 'sensitive' information (and how such information should be handled) are only amplified when looking across states.

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.

Issue 3 – 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. Most states cited current laws and agreements related to TB cases as a model for expanding to all other public health related conditions.

Issue 4 – 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) are also national-level issues, as they refer to federal requirements and regulations that would need to be looked at in order to address the issues.

Issue 5 – 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.

Issue 6 – Family Educational Rights and Privacy Act (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.

Issue 7 – 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.

Issue 8 – 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 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.

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

Overall, a number of valuable common themes can be constructed from the various state- and national-level issues identified on the HISPC Variations reports affecting Public Health.

The following table provides a summary of themes, identified state and national issues and possible consortium roles, opportunities and areas of work.

Table 1
Themes, Identified State and National Issues and Possible Roles, Opportunities and Areas of Work For the Consortium

Core Themes	Summary of Identified State and National Issues	Possible Consortium Roles, Opportunities and Areas of Work
Need to Develop a Public Health Privacy and Security Framework	■ Lack of a privacy and security framework that would apply to public health participation in RHIOs and local, state, regional and national health information exchanges	■ Convene a multi-stakeholder workgroup to develop such framework ■ Facilitate the convening of public health privacy officers, in partnership with ASTHO, NACCHO and others
Need to Advance Health IT Adoption in Public Health	■ Significant continued reliance on paper-based processes for public health information exchanges was common across states	■ Identify opportunities where state and local public health can move from paper to electronic
Need to Address Variations in Privacy and Security Policies and Practices Related to the Collection, Use and Disclosure of Health Information by Public Health	■ Variations around the reporting of communicable diaseases/notifiable conditions ■ Variations in the definition of 'Sensitive' health information ■ Level of access by public health agencies to health information during emergency, bioterrorism ■ Variations in the exchange of data with health oversight agencies when broad statutory authority exists	■ Prioritize areas of work (from list of identified items) and convene workgroup(s) to address the issues

Core Themes	Summary of Identified State and National Issues	Possible Consortium Roles, Opportunities and Areas of Work
	■ Variability of re-disclosure policies and practices applicable to public health agencies within state and across states	
Need to Advance the Adoption of Data Standards Related to the Collection, Use and Disclosure of Health Information by Public Health	■ In areas such as communicable disease reporting, disease registries, 'sensitive' information	■ Identify data standardization priorities and opportunities and work with Consortium's Data Standards Committee to address them
Need for Continued Education and Outreach	■ On a public health privacy and security framework ■ On the advancement of health IT adoption by public health ■ On the adoption of data standard and harmonized policies and practices related to the collection, use and disclosure of health information by public health ■ On the differences between voluntary vs. authorized vs. mandated exchanges of health information with public health agencies ■ On the interactions between federal and state laws affecting public health information exchanges ■ On targeted issues, such as how to address FERPA limitations to allow sharing of immunization data collected by schools	■ Prioritize and implement education and outreach activities through the Consortium's Education Committee