

June 30, 2007

# Privacy and Security Solutions for Interoperable Health Information Exchange

## Assessment of Variation and Analysis of Solutions Executive Summary

Prepared for

**Jonathan White, MD, Director of Health IT**  
Agency for Healthcare Research and Quality  
540 Gaither Road  
Rockville, MD 20850

**Jodi Daniel, JD, MPH, Director**  
**Steven Posnack, MHS, MS, Program Analyst**  
**Office of Policy and Research**  
Office of the National Coordinator  
330 C Street SW  
Switzer Building, Room 4090  
Washington, DC 20201

Prepared by

**Linda L. Dimitropoulos, PhD**  
RTI International  
230 W Monroe, Suite 2100  
Chicago, IL 60606

Contract Number 290-05-0015  
RTI Project Number 0209825.000.007



# Privacy and Security Solutions for Interoperable Health Information Exchange

## Assessment of Variation and Analysis of Solutions Executive Summary

June 30, 2007

Prepared for

**Jonathan White, MD, Director of Health IT**  
Agency for Healthcare Research and Quality  
540 Gaither Road  
Rockville, MD 20850

**Jodi Daniel, JD, MPH, Director**  
**Steven Posnack, MHS, MS, Program Analyst**  
**Office of Policy and Research**  
Office of the National Coordinator  
330 C Street SW  
Switzer Building, Room 4090  
Washington, DC 20201

Prepared by

**Linda L. Dimitropoulos, PhD**  
RTI International  
230 W Monroe, Suite 2100  
Chicago, IL 60606

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

## EXECUTIVE SUMMARY

This report is the fourth in a series to be produced under RTI International's contract with the Agency for Healthcare Research and Quality (AHRQ). The contract, entitled Privacy and Security Solutions for Interoperable Health Information Exchange, is managed by AHRQ and the Office of the National Coordinator for Health Information Technology (ONC). The following report is a summary of 34 separate final reports submitted by 33 states and one territory as subcontractors to RTI; these subcontractors form the Health Information Security and Privacy Collaboration (HISPC).<sup>1</sup> The Assessment of Variation and Analysis of Solutions (AVAS) report comprises the final reports submitted by the 34 subcontracted state teams and represents a "final look" at the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange and potential solutions to those issues raised. This summary report captures the highlights from the 34 reports and presents some of the major crosscutting themes that have been raised during the state teams' discussions.

This summary report consists of 8 major sections:

- Background and Purpose
- Assessment of Variation
- Summary of Key Issues Raised by the State Teams in the Assessment of Variation
- Review of State Solution Identification and Selection Process
- Analysis of State Proposed Solutions
- National-Level Recommendations
- Moving States Forward Collectively
- Conclusions and Next Steps

### Background and Purpose

The purpose of the AVAS is to illustrate, in a descriptive report, the variations among the organization-level business practices, policies, and laws, related to privacy and security, as identified by each state team. The term *law* as used here refers to regulatory, statutory, or case law that serves as the primary driver behind a business practice. The AVAS reports also describe the process for identifying and proposing potential solutions, including an explanation of how state teams are evaluating and prioritizing the solutions and their feasibility. The information summarized in this report was provided by each of the state teams as a result of the work conducted by the Variations Work Groups (VWGs), Legal Work Groups (LWGs), and Solutions Work Groups (SWGs) of each participating state team. The information also forms the basis for the work being conducted by the Implementation

---

<sup>1</sup> Throughout this report the 33 states and 1 territory are referred to as the state project teams or as the state teams.

Planning Work Groups (IPWGs) as the state teams finalize their implementation reports. Although the AVAS reports are final, the work continues as the state teams work with stakeholders toward developing privacy policy and security standards to address the needs of their local communities.

Although each state team followed a core methodology, ample opportunity remained to tailor the process to meet the needs of each participating state and territory. The reports include a section that documents the process used to generate the set of organization-level business practices for each scenario, including outreach to the broader stakeholder groups, and a description of the membership and stakeholder representation of the VWGs, LWGs, and SWGs. Each state team followed an outline that provided an *a priori* categorization for potential solutions based on whether the potential solution effected a change in organization-level practice or policy, state law or regulations, federal law or regulations, or specifically impacted interstate electronic health information exchange. Although this categorization was recommended, state teams were given the opportunity to tailor the categorization to meet the needs of their specific participating state or territory. The reports also included a section in which state teams could discuss potential solutions that would require implementation at the national level. The outline and content of the AVAS reports are described in Table ES-1.

## **Summary of Assessment of Variation**

The descriptions of business practices in each of the HISPC reports are organized by 11 purposes for health information exchange (HIE), as shown in Table ES-2. These purposes represent clusters of the 18 scenarios used to drive the discussions of business practices. Within each of the 11 sections, each state team was asked to provide a description of (1) the stakeholders who provided input to the collection of business practices; (2) the major domains addressed by the business practices (based on the 9 domains of privacy and security) including a discussion of the relevant policy, legal drivers, or rationale behind the practices; and (3) critical observations not offered elsewhere in the report. Finally, each state report provided a summary of the critical observations and key issues that the SWGs and the IPWGs further explored.

## **Summary of Key Issues in the Assessment of Variation**

The AVAS report describes 10 major issues that state project teams raised as having broad implications for private and secure nationwide electronic health information exchange. This section provides a brief overview of these topics, which is not intended to be a thorough analysis of the issues or their implications, but rather a descriptive treatment of the issues.

**Table ES-1. Outline of Assessment of Variations and Analysis of Solutions Report**

<b>Section Title</b>	<b>Content</b>
Section 1—Background and Purpose	Purpose and scope of this report Description of level of health information technology (HIT) development in the state/territory Description of report limitations
Section 2—Assessment of Variation	Brief description of the methodology Description of variation identified, organized by scenario including stakeholders, domains, and critical observations
Section 3—Summary of Key Issues Raised by the State Teams in Assessment of Variation	Discussion of the key areas of variation as identified by the state teams
Section 4—Review of State Solution Identification and Selection Process	Description of the state Solutions Work Group, its charge, membership and stakeholder representation Description of the process the state used to identify and propose solutions Description of the process the state used to vet, evaluate, and prioritize solutions Description of how state determined the level of feasibility of identified solutions
Section 5—Analysis of State Proposed Solutions	Solutions to issues driven by variation in organizational business practices and policies (but not state laws) Solutions to issues driven by state laws/regulations Solutions to issues related to technology and standards Solutions to issues related to education Solutions to issues related to implementation and governance Solutions to collateral issues
Section 6—National-Level Recommendations	National standards related to draft model legislation, business agreements, uniform patient consent/authorization forms, national oversight body Clarification/revisions to federal regulations Funding
Section 7—Moving States Forward Collectively	Coordinating standards and policy Coordinating legislation
Section 8—Conclusions and Next Steps	Discussion of the implementation plans

**Table ES-2. Purposes of Health Information Exchange (HIE) and Relevant Scenarios**

<b>Purposes of HIE</b>	<b>Relevant Scenarios</b>
Treatment	Scenarios 1–4
Payment	Scenario 5
Regional health information organizations (RHIOs)	Scenario 6
Research data use	Scenario 7
Law enforcement	Scenario 8
Prescription drug use/benefit	Scenarios 9 and 10
Health care operations/marketing	Scenarios 11 and 12
Bioterrorism	Scenario 13
Employee health	Scenario 14
Public health	Scenarios 15–17
State government oversight	Scenario 18

***Variation in the Interpretation and Application of Consent versus Authorization<sup>2</sup>***

The state teams have identified broad variation in the use and implementation of patient consent and authorization. The terms are often used interchangeably although they have two distinct definitions and separate uses under various federal and state laws. For example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires patient authorization for any uses and disclosures of protected health information (PHI) not otherwise permitted or required by the Privacy Rule. In contrast, the Privacy Rule permits, but does not require, the obtaining of consent for uses and disclosures of PHI for treatment, payment, and health care operations purposes. Further, the term *consent* has a specific meaning pursuant to the provisions of 42 C.F.R. pt. 2 (alcohol and chemical dependency). Despite the specific legal definitions, the terms *patient consent* and *patient authorization* have been used *interchangeably* by some state teams to refer to the *need for* (perceived or otherwise) and the actual *process of* obtaining appropriate approval from a patient (who is the subject of the information) or a corresponding legal guardian or representative before use or disclosure of the patient’s health information. Included are specific discussions regarding consent for treatment, payment, and health care operations;

---

<sup>2</sup> The terms *consent* and *authorization* have specific meanings in the context of various state and federal laws. Although context must be considered when examining a specific statute, here the terms are used to generally mean a signed permission to release or disclose protected health information.

special rules for disclosure of sensitive information; and challenges ahead for devising an approach to managing permissions necessary to permit electronic exchange.

### ***Differing Interpretations and Applications of HIPAA Privacy Rule Requirements***

State teams reported many business practice variations based on different interpretations and applications of the requirements of the Privacy Rule. This variation was not unexpected and is the result of the intentional flexibility and scalability of some of the Privacy Rule's requirements (eg, *minimum necessary* and reasonable safeguards). The most commonly mentioned issues were variability in application of the *minimum necessary* standard and the use and implementation of patient consent, which the Privacy Rule permits but does not require, or authorization, across organizations.

### ***Misunderstandings and Differing Applications of the HIPAA Security Rule***

The state teams indicated that stakeholders misunderstood and were confused about appropriate security practices; moreover, they also misunderstood what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust among organizations and stakeholders was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule.

## ***Security***

***Authentication and Authorization.*** A number of state teams identified the need for standard authentication and authorization protocols to permit electronic health information exchange. State teams noted that the lack of a common method for authenticating individuals created mistrust between organizations. Currently, some organizations will accept a phone call or a fax from a known staff member at the requesting organization to authenticate the request and disclose the information. This is typical if the organizations have a previously established relationship. However, the same organization may impose a stricter requirement on other organizations including the requirement that the patient or individual sign a consent form (although not necessarily required by law) before the personal health information is exchanged. It becomes a cumbersome process that does not lend itself well to electronic health information exchange.

***Inadequate Application-Level Data Access or Screening Controls.*** The state reports clearly indicate that many stakeholders are not using or are not familiar with currently available technologies. A critical issue identified by stakeholders that are either current users or exploring available technologies are the inadequacies in existing applications used to manage personal health information and for HIE, including electronic health records (EHRs) and data repositories. For example, some stakeholders indicated that they were required to print out copies of records from EHRs and redact especially sensitive

information, or information that should not otherwise be disclosed, because the EHRs did not accommodate segregation of certain types of data. The current business practice is to print a paper copy, redact the information, and fax the redacted copy of the record to the intended recipient.

***Audit Programs.*** Several state teams indicated that the poor auditing capability of current software applications is a challenge to electronic health information exchange and that it is particularly problematic when the management of community health records or HIEs was discussed. Adequate audit processes mean more than activating the appropriate audit logs; they include the development and regularly scheduled use of an appropriate audit program that addresses potential privacy and security risks and is based on an established set of audit criteria that match the organization's needs.

***Secure Transmission of Personal Health Information.*** Several state teams identified the secure transmission of personal health information between health care organizations, and between health care organizations and consumers, as a significant issue. Reports cited the lack of interoperable solutions and the high cost of implementing appropriate forms of secure transmission that protect the data in transit and protect against inappropriate interception and potential modification.

***Lack of a Sound Security Infrastructure.*** A number of the state reports addressed interorganizational security issues but did not examine barriers related to these issues (administrative, physical, and technical). The lack of appropriate security program investment by health care and related organizations stems generally from 3 areas that should be reviewed and addressed at the organizational, state, and federal levels, including lack of knowledge about appropriate security practices and HIPAA Security Rule requirements; lack of investment in security on the part of the industry; and the method by which the HIPAA Security Rule is enforced by the US Department of Health and Human Services.

***Variability in Administrative and Physical Safeguards.*** State teams noted that the lack of adoption of consistent and appropriate administrative and physical safeguards within health care organizations has resulted in mistrust between organizations and increased concerns related to liability (where an organization with a sound security program transmits personal health information to an organization that lacks a sound security infrastructure). This issue is not related to technology; rather, it involves lack of understanding about, or insufficient emphasis on, appropriate security for any size organization. State teams noted that reducing the variability in the application of administrative and physical security would do much to reduce certain challenges to electronic health information exchange, improve trust among organizations, and reduce liability concerns.

### ***Trust in Security***

Providers were principally concerned about potential liabilities from the activities of other participants in electronic health information exchange and about consumers' lawsuits for errant or inappropriate disclosures of their information. One state identified the concern about trust as the single most significant issue, one which had been repeatedly raised by stakeholders and the reason providers were not willing to participate in HIEs.

The second most commonly reported trust issue was consumer lack of trust in electronic health information exchange. The primary concern consumers raised was related to payer and employer access to health data and, secondarily, distrust of new technologies.

### ***State Laws***

Organizations vary widely in how they identify, locate, and apply existing state law. Some organizations use the HIPAA Privacy Rule as a ceiling rather than as the federal floor. In many states, the relevant state law is fragmented and scattered throughout many chapters of state law, making it difficult to find. In addition, the laws frequently conflict, are antiquated, and do not apply to electronic health information exchange.

### ***Networking Issues***

Most state teams were concerned about the lack of well-defined, operational, and deployable models for regional networking, which created a gap between policy development and practical application; in some states, this gap made it difficult to engage stakeholders in the policy work.

### ***Linking Data from Multiple Sources to an Individual***

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to electronic health information exchange. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use and disclosure of personal health information, and inappropriate clinical decision-making issues that are both a clinical and a privacy risk.

### ***Interstate Exchange Issues***

Although the identification of interstate issues was not a primary focus of the interim assessment of variation, more than half the state teams reported that interstate issues should be considered and that agreements among states must be made to facilitate the exchange. States typically raised interstate issues because health care facilities draw patients from across state lines or because states experience very large seasonal inflows of both out-of-state workers and tourists.

### ***Disclosure of Personal Health Information***

The state teams reported multiple sources of variation in business practices related to the disclosure of health information:

- multiple interpretations of the requirements for patient consent or authorization in connection with the release of health information;
- issues related to the re-release or redisclosure of health information received by one entity from another;
- differences in how sensitive health information is treated;
- multiple interpretations and applications of the HIPAA Privacy Rule *minimum necessary* requirement;
- issues about rights and responsibilities regarding control of health information;
- varying degrees of reporting requirements for public health purposes;
- issues of ownership of health information;
- need for fast, easy, and secure electronic health information exchange under medical or health emergency circumstances;
- handling of disclosures related to judicial proceedings and law enforcement; and
- burden imposed by the need to document certain disclosures of health information.

### ***Cultural and Business Issues***

State teams referenced cultural and business issues that pose challenges to electronic health information exchange.

- Stakeholders are concerned about liability for incidental or inappropriate disclosures, which causes many organizations to take a conservative approach to developing practice and policy.
- A general resistance to change is evident; organizations and individuals are comfortable with existing paper-based or manual systems believed to be timely and effective.
- Clear definitions of terms within state and federal laws are needed. For example, terms like *medical emergency*, *current treatment*, *related entity*, and *minimum necessary* do not have agreed-upon definitions and, therefore, serve to increase variation.
- Tension exists among health care providers, hospitals, and patients concerning who controls or owns the data.

### **Review of the Solution Identification and Selection Process**

A number of factors affected the approach that each state team took to developing solutions to the challenges and barriers to private and secure electronic health information exchange. Teams that represented states with existing HIEs or states that have done significant work toward implementing electronic health information exchange provided some very detailed

and specific analyses of the technical issues related to data security and standards. Teams representing states in the early stages of planning for electronic health information exchange tended to focus more on understanding the sources of variation that were identified; making decisions about the role of human judgment and how to build trust into the system; and developing governance structures and the need for oversight bodies and funding. Other factors also contributed to the variation in the reports, including the level of fragmentation of state laws. States with highly fragmented state privacy law focused on resolving that source of variation while states with relatively little or no state law governing privacy and security of electronic health information exchange discussed the possible need for legislation. On the other hand, some state teams with fairly stringent state privacy laws discussed the potential need to make changes to permit electronic health information exchange. Their struggle is the balance between ensuring the privacy and security requirements of their communities and maximizing the benefits of electronic health information exchange to the community.

## **Summary of Solutions**

While many of the identified solutions were specific to a state, a number of common themes, issues, and solutions clearly surfaced. Generally, states' solutions fell into one or more of the following broad common areas that serve as a source of variation.

### ***Reducing Variation: Practice or Policy Solutions***

State teams identified the greatest amount of variation in organizations' interpretation and application of the HIPAA Privacy and Security Rules, including its *minimum necessary* standard. The Privacy Rule is frequently cited as limiting exchange, even though it generally allows the use or disclosure of protected health information, without *authorization*, for treatment, payment, and health care operations. All state teams agree that to reduce the current existing variation that poses challenges to interoperable electronic health information exchange, organizations and states must agree on some common interpretations and applications of the HIPAA Rules and develop some uniform policy. In addition to broad agreement on the need for policy development, the state teams also advanced many specific recommendations for detailed policy development. The state teams agreed on the need to define parameters for standard use and disclosure, including specifying the purpose and use of the data, consent and authorization policies and procedures, data use limitations, data collection limitations, and requests for restrictions on data use and disclosure, patient notification (including accounting and audit of prospective and retrospective data uses and disclosures), and patient education (including information about patient rights, granting of consent, and others). State teams also agreed about the need to establish a standardized or uniform patient consent form and process to be adopted by the entire health care industry. A number of states indicated that the uniform consent form and policy should clearly reflect patients' rights to information in their medical records

and provider confidentiality principles. Another state team added that state law should determine general consent requirements, consent principles relative to condition-specific consent requirements, interstate information exchange, information exchange with payers and employers, use of information for marketing, and waivers of consent when the patient's life is at risk and in public health emergencies.

### ***Legal or Regulatory Solutions***

Four state teams identified another source of variation driven, in part, by difficulties identifying and interpreting state law that is frequently fragmented and scattered. In addition, once found, the laws sometimes conflict with one another. This situation is further complicated by misunderstanding of how the state law intersects with federal laws and regulations. A number of state teams have proposed plans to consolidate statutes related to HIE to facilitate review to identify conflicting or outdated state laws.

State teams were also concerned about restrictive or outdated state laws that currently do or may in the future govern private and secure electronic health information exchange. Many states have no clear comprehensive privacy approach or any current body of state law governing electronic health information exchange. A number of state teams noted the need to update state laws and regulations to address provisions that inadequately address interoperability of electronic health information exchange and to reconcile the differences between state laws and the Privacy Rule. Some specific recommendations that should be included in a comprehensive approach include exploring the creation of new laws/policies to protect health care information held by third-party custodians. State teams also recommended amending existing laws/policies to ensure patients have access to their health information in electronic format, where available. One state specifically proposed making modifications to state statutes to resolve differences regarding *when* and *how* patient consent is required to exchange patients' health information. The team also identified the need to define undefined terms and ambiguous concepts in state patient consent requirements (such as *health record*); add language to clarify application of the state's patient consent requirements to new concepts in electronic health information exchange; and update the state's patient consent requirements to allow mechanisms that facilitate the electronic exchange of patients' information while respecting patients' ability and wishes to control their information.

Additional recommendations include the following:

- Draft sample language for uniform medical records statutes and regulations.
- Develop/promulgate rules detailing electronic health information exchange during a bioterrorism response and action, including public/private electronic health information exchange.
- Examine the federal and state provisions governing responsibilities to maintain and control patient data and records.

- Draft new legislation that provides specific protection for genetic data and that would standardize the age of consent regarding the release of medical information for treatment, payment, and operations to permit interstate exchange.
- Revise statutes to address electronic health information exchanges in emergency situations where the patient is unable to provide written or verbal consent.
- Request state regulatory change to include state versions of an exception to patient consent for treatment, payment, and health care operations.
- Evaluate the feasibility and applicability of a model state law or model state contract for the privacy and security of health information and, if appropriate, work with other states to develop and recommend such models.
- Require state government to recognize the Healthcare Information Technology Standards Panel (HITSP) and the Certification Commission for Healthcare Information Technology (CCHIT) standards criteria for privacy and security in all relevant contracting, policies, and programs.

Recommendations were also offered to address differences between state and federal laws dealing with inconsistent and sometimes conflicting requirements for patient consent; disclosure of sensitive health information; security requirements such as data protection, including business agreements, authentication, authorization of all individuals and their delegates; protection of data at rest in each party of an exchange; and protection of data in transit.

Similarly, a number of state teams identified the need to address inconsistencies between federal and state laws and regulations in areas such as sharing of specially protected health information (eg, mental health and substance abuse data); Medicaid data sharing; interstate data sharing; state-to-local data sharing; data sharing for research; and data sharing in an HIE.

### ***Technology/Data Standard Solutions***

A number of state teams proposed the development of a standard national data format to document consent that recognizes the differing state-based consent policies, laws, and regulations but also promotes normalization and common application. In addition, a number of state teams, citing the need for patients to have more control over access to their health records, recommended that higher access standards/restricted access standards be developed for select information. These teams also indicated a need to educate patients on how, when, and why to control access to their information. Another recommendation was that states develop mechanisms and standards under which patient notification and a full audit trail is provided when specially protected information is requested and accessed.

A number of states proposed solutions for managing patient identity. The ability of a health care provider to identify the correct records for a patient is critical to clinical medicine and to electronic health information exchange. The lack of a standard, reliable way to accurately match records to patients introduces the potential for inappropriate use or disclosure of

health information about the wrong patient, both a clinical and a privacy risk. This problem is particularly acute when information is shared across institutions that have different methods of patient and record identification. All state teams noted the need for the ability to correctly identify patients, and most states recommended potential ways to accomplish this goal. Some recommendations include:

- Develop national guidelines and standards for a master patient index or record locator service.
- Establish a patient identity management service.
- Adopt a universal standard for patient identification, with official, verifiable means of both primary and secondary identification defined.
- Identify and adopt standards on patient identification (including unique patient ID, record locator capabilities, access to personal information, and ability to amend portions of the record).
- Identify and use a unique identifier for patient identification, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier.
- Identify patients accurately through biometrics.
- Coordinate a statewide approach to identify, authenticate, and authorize patients.

A number of state teams reported the need for systems that can segregate data to allow for controlled access to specially protected data and to allow patients to control access to portions of their records.

### ***Education***

All states recognize the need for varying levels of education to reduce variation in how policies are applied and also to increase stakeholder awareness and trust in the systems. The most common recommendations were for educational campaigns directed at patients and consumers and training programs for providers and organizations. Some examples include:

- Educate patients and consumers concerning federal and state privacy laws at both the national and state level. Include an explanation of the conditions in which their individually identifiable health information can be disclosed without their permission.
- Conduct a consumer needs assessment to see what consumers most want from an electronic health record (EHR)/HIE environment; focus on providing these functionalities to encourage public acceptance.
- Establish core education competencies for staff who manage personal health information, to include not only privacy and security training, but also awareness of the technical issues relevant to their job responsibilities and electronic health information exchange.

## ***Implementation and Governance of Solutions***

One goal of this project is to establish a state infrastructure that will allow the work to continue beyond the conclusion of this contract. To that end, a number of state teams have proposed an administrative or governance body to oversee the state's electronic health information exchange activities. Some recommendations are overarching to include all activities related to electronic health information exchange advancement and define the source of authority, operational structure, rules of the governing body, rules of participation in an electronic health information exchange network, and service offerings of the oversight entity. Other state teams propose forming entities to govern specific areas. For example, some state teams have proposed the establishment of an HIE Privacy and Security Advisory Board to oversee key aspects of privacy and security for statewide HIE. States also proposed establishing an information technology privacy and security committee to recommend standard privacy and security policies, procedures, and technology controls. Some states also suggested the formation of legal committees to recommend legal solutions to privacy and security issues.

## ***Ancillary Issues and Solutions***

***Funding.*** A few states recommended investigating the possibility of providing public and private financial incentives for organizations to implement best security and privacy practices. Many more states explored ways to fund electronic health information exchange activity in the broader context, including providing incentives for adoption of technology. Although not directly related to the development of privacy policy and security standards, the funding and adoption issues are closely related to maintaining momentum among stakeholders working on the policy issues. A few examples are included below:

- Utilize tax incentives and other state-supported financing mechanisms for providers to invest in technology that will advance the utilization of private and secure HIE methodologies and systems.
- Research opportunities to make the HIEs reimbursable by Medicaid and under the state employee group health plan.
- Provide financial support for electronic health information exchange activities through grants, fundraising, and government appropriations.

***Incentives/EHR Adoption.*** Financial incentives are an obvious solution to EHR adoption issues. Small providers, those located in rural or low-income areas, or providers with a large percentage of underinsured or uninsured patients, may face financial difficulty in purchasing and implementing EHR systems. The state teams proposed several types of incentives including tax incentives for providers, combinations of private and public incentives, and incentives for organizations that implement best practices in privacy and security. State teams also considered nonfinancial incentives, including a proposed mentoring program for providers who are implementing EHR systems.

**Stakeholder Engagement.** Although each state team is composed of representatives from a broad array stakeholders, all teams recognized the need for the continual engagement of stakeholders in discovery and solution development. Clearly, all state teams understood the need for ongoing consumer participation. A few examples of plans for engaging consumers are as follows:

- Hold a community forum.
- Assess consumer needs.
- Determine consumer perceptions and understanding of specially protected clinical data to see if it aligns with state and federal law.
- Strengthen the communication channels between the state, Indian Health Service, and sovereign Native American tribes.

In the majority of cases, stakeholder engagement included some form of educational programs.

## **Summary of National-Level Recommendations**

The final section of the report summarizes the state teams' recommendations for solutions that would be most effectively implemented at the national level. The state project teams focused primarily on generating potential solutions that could be implemented at the local or state level. However, state teams also recommended solutions at the federal level that would be highly valuable to states as they develop privacy policy and security standards. Many ideas summarized in this section were also raised by other state teams as potential solutions to be implemented at the state level. The state teams that offered these preliminary thoughts about national level recommendations generally indicated that privacy policy and security standards for electronic health information exchange could achieve faster uptake if adopted at the national level rather than trying to come to agreement nationwide at the state level.

### ***National Standards***

Many state teams called for national standards to form a framework for nationwide electronic health information exchange. The teams recommended standardizing both a basic set of data elements and the accompanying technical standards for the interstate transfer of personal health information. All state teams expressed an interest in sharing data across state lines; however, some state teams felt strongly that the federal government would need to impose a national framework as a starting point that would include national standards that the states could use as a common basis for exchange. These state teams argued that without a national framework, the states will develop silos that will not be able to exchange data with one another, leading to a fragmented and disjointed system. Some state teams also noted that, while technical solutions can be designed and implemented at a regional level, they can lead to multiple and disparate approaches that would inhibit

exchange among regions. National standards and guidelines could provide a platform to begin exchange discussions; states could alter it if necessary, but a similar core framework would be maintained from state to state. Similar arguments were proposed for the development and publication of a national standard for data sharing agreements.

**National Standards for Transferring Health Information Among States.** State teams most frequently called for national standards that would collectively guide the transfer of health information among states. Without a centralized effort, states could go in disparate directions or the effort will take far longer to coordinate.

**National Standard for Health Information Exchange-Related Business Associate Agreements.**<sup>3</sup> Similar arguments were proposed for the development and publication of a national standard for data sharing agreements, such as a business associate agreement (BAA).<sup>4</sup> Eight state teams proposed that a standard BAA be established at the national level even though there is a national standard for BAAs and data use agreements in the HIPAA Privacy Rule.

**Standardized Model National Consent Form.** The state teams indicated that a model consent form is one of the essential components to encourage data sharing among organizations and across states. Many state teams have proposed solutions about the development of statewide uniform consent models. State teams recommending a model national consent form recognize that each state must be concerned with the unique state laws that affect their consent process, but they also recognize that using a common template to build upon will decrease variation.

**Centralized Model Regulation Process.** To develop a centralized model regulation development process, state teams suggested a range of options: a national effort to provide structured guidance to the current national standard setting bodies, a centralized national process to examine the role of emerging standard setting organizations, and working with the National Conference of Commissioners on Uniform State Laws (NCCUSL) to broker a set of model legislation. All states proposing this recommendation felt that some national-level oversight was needed in the production of model standards or model legislation.

---

<sup>3</sup> Five of the 8 states making this recommendation referred specifically to a national standardized business associate agreement, and 3 state teams referred to contractual or participant agreements. None of the states used the more specific term *business associate contract*. HIPAA requires covered entities to document they have obtained satisfactory assurance that their business associate will safeguard health information through a written contract or other written agreement or arrangement. The Privacy Rule has specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memorandums of understanding between agencies. Thus, the term *business associate agreement* encompasses both contracts and other arrangements, so this term is used in the summary above.

<sup>4</sup> These types of agreements are common and required by both the HIPAA Privacy and Security Rules. BAAs are executed whenever a third party performs certain services for a covered entity that includes access to PHI. For example, organizations receiving PHI and serving as a platform for many regional or local data exchange systems on behalf of covered entities would be a business associate of all covered entities that use the organization's services.

**National Oversight Body.** Three state teams proposed that an organized authority or oversight body guide the standardization of privacy and security implementation among states. Although all 3 states provided different alternatives, the sentiment was that this oversight could accelerate the adoption of recognized model laws, contracts, policies, and procedures among participating entities in an HIE. The state teams also recommended that the national oversight body oversee a consistent national educational campaign to consumers that will lead to greater public understanding and electronic health information exchange participation.

### ***Clarifications/Revisions to Federal Regulations***

The second most frequent set of issues raised by the state teams that offered national-level recommendations included recommended revisions and clarifications to federal regulations, including HIPAA Privacy Rule, 42 C.F.R. pt. 2, Clinical Laboratory Improvement Amendments (CLIA) regulations and Medicaid data disclosure regulations.

**HIPAA Privacy Rule Revisions/Clarifications.** Only 6 state teams recommended clarifications or revisions to the HIPAA Privacy Rule. One state team stated that clarification and perhaps revision of the Privacy Rule is necessary to reduce the variation in interpretation and application of Privacy Rule provisions across organizations and states.

Two states recommended that the Privacy Rule requirements for *minimum necessary*, de-identification, limited data set, and designated record set be reviewed for possible technical adjustments. Neither state elaborated on what types of technical adjustments were recommended, nor did they describe in the interim report what was problematic. Both state teams also recommended that the Department of Health and Human Services (DHHS), Office for Civil Rights, develop new and more nuanced guidance.

One state pointed out the need to clarify appropriate electronic exchange guidelines to provide specific guidance concerning federal law restrictions about information types and classes, and also to provide solutions by which electronic personal health information can be viewed and exchanged outside established HIPAA standard transactions (eg, via EHR, electronic clinical notes, electronic health information exchange, and so forth).

One state team identified 3 potential changes to the Privacy Rule to reduce both administrative burden and variation. First, the state team noted that although the Privacy Rule introduced requirements intended to protect patient privacy, in some situations, the requirements provide nominal improvements in patient privacy protections over existing state law but increase administrative burdens in ways that may impede electronic health information exchange. The team's first proposed solution was to remove the requirement for BAAs and modify the statute to hold business associates directly accountable and liable for adhering to the Privacy Rule requirements. Second, the state team explained that interpretations and applications of the *minimum necessary* standard vary widely. The team

proposed that states work to develop model policies and procedures to promote more consistent application of the *minimum necessary* standard. Finally, the team noted that prior to the HIPAA Privacy Rule, access to research information without patient consent was controlled by 45 C.F.R. pt. 46, the Common Rule, which applies to all research on Human Subjects. The Privacy Rule's requirements governing access for research purposes are deemed more protective of patient information than state laws; therefore, the Privacy Rule requirements control access without consent for research purposes. Under the Privacy Rule, generally, if researchers request access to identifiable health information as part of a research study, they must either obtain a waiver of *authorization* from the institutional review board (IRB) as part of the IRB approval process, or obtain *authorization* from all patients in the study.<sup>5</sup> Because of the additional waiver criteria required by the Privacy Rule, many facilities have created privacy boards in addition to the IRB to evaluate and grant waivers. In evaluating a research proposal, an IRB is required to weigh the proposal's risks and benefits, including its impact on the confidentiality of patient health information. The state team agreed that IRB approval under the Common Rule is sufficient to protect patient confidentiality, and the team proposed that the federal government eliminate the Privacy Rule's additional waiver criteria.

***Clarify Legal Status under HIPAA of Entities Participating in an HIE.*** Two state teams noted a need to clarify the legal status of certain entities participating in HIEs, including regional health information organizations (RHIOs), and to clarify whether they could be considered covered entities, business associates, or another as yet undefined category. The state teams noted a need to adopt a nationally accepted common definition of terms when referring to these organizations, their organizational and structural models and core components, their operational frameworks, and their legal standing in terms of liability.

***Confidentiality of Alcohol and Drug Abuse Patient Records (42 C.F.R. pt. 2).*** Seven state teams raised issues related to 42 C.F.R. pt. 2, and 3 state teams proposed ways to manage the special protections governing the exchange of information that is protected by the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 C.F.R. pt. 2).<sup>6</sup> Two state teams proposed adopting technological solutions (such as using the continuity of care record to restrict transmission of specially protected data). Three other state teams proposed legislative or regulatory changes that may not be feasible but, nevertheless, highlight areas with which the state teams are struggling, including:

- Amend 42 C.F.R. pt. 2 to state that patient consent is not required to exchange the data for treatment purposes and impose strict monetary penalties for misuse or inappropriate disclosure of identifiable alcohol or chemical dependency data (that would require appropriate and consistent enforcement activity). Currently, the criminal penalty under 42 U.S.C. §§ 290ee–3(f), 290dd–3(f), is that any person who

<sup>5</sup> 45 C.F.R. § 164.512(i)(2)(ii).

<sup>6</sup> 42 C.F.R. pt. 2 uses the term *alcohol and drug abuse*. Most of the states used the term *substance abuse*. This summary has adopted the terminology from the federal regulation for consistency.

violates any provision of the statutes or regulations can be fined not more than \$500 in the case of a first offense, and not more than \$5,000 in the case of each subsequent offense.

- Explore DHHS's authority to define the contours of the consent without the need for legislative action, recognizing that it may not be permitted without Congressional action. That is, the consent provisions should be clarified so that a single consent allows for unlimited downstream releases for certain purposes (eg, treatment), clarify that consent can describe generally the entities to which pt. 2 records may be disclosed (eg, health care providers), and also allow consent to be effective indefinitely—at least until explicitly revoked.

***Revision or Amendment to CLIA Regulations.*** One state suggested a revision to the federal CLIA regulations. The federal CLIA regulations, 42 C.F.R. § 493.1291(f), currently provide as follows: "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." The term *authorized person* is defined in 42 C.F.R. § 493.2 as "an individual authorized under State law to order tests or receive test results, or both." The term "individual responsible for using the test results" is not defined in the CLIA regulations, and its meaning is uncertain. The state team proposed that the CLIA regulations may pose a barrier to laboratories' exchange of health care information directly with the patient, with RHIOs, or with other similar organizations who may participate in electronic health information exchange.

### ***Funding***

***Funding for More Widespread Adoption of Technology.*** Although this project focuses on issues related to private and secure electronic health information exchange, nearly all states raised the issue of low levels of technology adoption and the absence of a technical infrastructure as key barriers to their progress with the privacy and security work. Two state teams reported that national-level incentives could help sustain the momentum and prevent discussions from stagnating.

***Funding for Educating Patients and Consumers.*** Two state teams called for education campaigns at the national level to reduce variation in practice. One state called for a national DHHS public relations effort to provide a consistent, centralized, and visible source of education to the public.

### **Moving States Forward Collectively**

The primary goal of each state team was to work toward solutions that would enable secure and private transfer of electronic health information between entities. However, the importance of collaboration in this project should not be ignored. Perhaps the greatest long-term effect of these activities will be the concurrent momentum built within each of the subcontracting states, the enthusiasm of which was not confined to state lines.

## **Conclusions and Next Steps**

While the national-level recommendations summarized in Section 7 are an important outcome of the project, the final effort will focus on developing implementation plans for the state/territory-level solutions summarized in Section 5. These have been classified into 6 types of solutions:

- reducing variation: practice or policy solutions;
- legal and regulatory issues;
- technology and data standards;
- education;
- implementation and governance of privacy and security solutions; and
- ancillary issues and solutions.

The implementation plans for each of the state teams have been emphasized from the project's initiation. The project teams in each state and territory have been reminded that the government's purpose in funding this project has been not only to identify barriers to electronic health information exchange but also to solve them in a way that protects the privacy and security of health care consumers. The project has generated much discussion over the course of the past 10 months in steering committees and work group sessions, in stakeholder meetings, and in the regional meetings—as well as at the national meeting that was held in March 2007. These discussions have, in turn, resulted in stakeholders' commitments to fulfill the promises of improved health information exchange and to protect this information. In addition to a better understanding of barriers and proposed solutions, the perpetuation of this commitment is a major goal of the collaboration.

In developing their implementation plans, the state teams have been encouraged to focus on the practical and efficacious. As noted previously, conditions relevant to electronic health information exchange vary both within and between states. What works in one state may not work in another. The project teams have been encouraged to vet implementation plans with stakeholder groups in the same iterative process used to identify the variation in business practices, policies, and state laws to develop solutions that reduce variation and permit widespread electronic health information exchange in a private and secure way.

Based on the draft implementation plans provided by the teams in each state/territory, we anticipate the final implementation plans will include detailed plans to move forward in the following areas:

- governance and leadership;
- business practices and policies;

- legal and regulatory solutions;
- technological and data standards solutions; and
- education and outreach.

In addition to these concrete objectives, the project teams in each state/territory have provided practical considerations for accountability, funding, and specific timelines.