July 20, 2007

Privacy and Security Solutions for Interoperable Health Information Exchange

Nationwide Summary
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 0209825.000.009

RTI Project Number 0209825.000.009

Privacy and Security Solutions for Interoperable Health Information Exchange

Nationwide Summary
Executive Summary

July 20, 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

List of Authors for Summary Report

Amoke Alakoye, MHS, RTI International
Holt Anderson, Executive Director, NCHICA
Chris Apgar, CSSP, CISSP, Apgar & Associates
Alison Banger, MPH, RTI International
Ryan Bosch, MD, George Washington University Medical Faculty Associates
Robert F. Bailey, BA, RTI International
William Braithwaite, MD, PhD, Braithwaite Healthcare Consulting
John Christiansen, Christiansen IT Law
Gary Christoph, PhD, CIO, Teradata
Linda L. Dimitropoulos, PhD, RTI International
David H. Harris, MPH, RTI International
Mike Hubbard, Womble, Carlyle, Sandridge & Rice, PLLC
Cynthia L. Irvin, PhD, RTI International
John Loft, PhD, RTI International
Barbara L. Massoudi, MPH, PhD, RTI International
John McKenney, SEC Associates
Anna Orlova, Public Health Data Standards Consortium
Harry Rhodes, MBA, RHIA, CHPS, AHIMA
Stephanie Rizk, MS, RTI International
Joy Pritts, PhD, Health Policy Institute, George Washington University
Walter Suarez, MD, CEO, Institute for HIT/HIPAA Education and Research
Michelle Lim Warner, MPH, Center for Best Practices, National Governors Association

EXECUTIVE SUMMARY

This report presents an overview of the work conducted by 33 states and Puerto Rico under the Privacy and Security Solutions for Interoperable Health Information Exchange contract funded and managed by the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology (ONC).

Scope and Purpose of the Nationwide Summary

The purpose of this Nationwide Summary report is to provide a comprehensive review of the work conducted by the state teams[1] throughout the course of this project. Although the primary sources of information described in the Nationwide Summary report are necessarily state-specific, the report affords the opportunity to look across the activities conducted by the 34 state teams and to better understand what policies and practices need to be in place within and across states to both protect health information and promote nationwide electronic health information exchange. This Nationwide Summary report is an effort to expand the ideas and plans the state teams have developed by identifying common challenges and areas for ongoing collaboration. The Nationwide Summary report also incorporates issues raised during discussions at the regional and national meetings and presents discussions of key issues, based on the expertise of the members of RTI's Technical Advisory Panel (TAP) regarding the often complex interactions between state and federal law. This report addresses the broader implications of the project, makes recommendations for federal action that can facilitate nationwide electronic health information exchange, and may serve as a roadmap for state and federal agencies establishing privacy and security policies governing nationwide electronic health information exchange.

The work represented in this report was conducted by project teams in the 33 states and Puerto Rico, which form the Health Information Security and Privacy Collaboration (HISPC) project. Although the landscape for privacy and security in the remaining states and territories likely has some unique characteristics, most of the issues discussed in this report cut across the entire nation.

Overview of the Privacy and Security Contract

In June 2005, the US Department of Health and Human Services (HHS) published the *Summary of Nationwide Health Information Network Request for Information Responses,* which contained responses from 512 organizations and individuals. In this report, privacy and security considerations were crosscutting, and nearly every response cited the importance of "patient privacy and reiterated that the American public must feel confident that their health information is secure, protected, portable, and under their control" (p. 21).

[1] Throughout this report the 33 states and 1 territory are referred to as the *state project teams* or as the *state teams.*

The report also noted major concerns among respondents about the varying applications and interpretations of the HIPAA Privacy and Security Rules being implemented by organizations and the challenges this variation would pose to nationwide electronic health information exchange. Respondents noted that the HIPAA Privacy and Security Rules allow for 2 hospitals to develop 2 different business practices, both compliant, for protecting privacy and security of health care records, and that this variation must be addressed if interoperable electronic health information exchange is to be achieved nationwide. Furthermore, the respondents noted that complications would occur both within and across states because of inconsistencies and differences between state privacy laws and federal laws.

The purpose of this Privacy and Security Solutions for Interoperable Health Information Exchange project has been to assess variations in organization-level business practices, policies, and state laws that affect electronic health information exchange and to identify and propose practical ways to reduce the variation to those "good" practices that will permit interoperability while preserving the necessary privacy and security requirements set by the local community.

Formation of the HISPC

The Health Information Security and Privacy Collaboration (HISPC) comprises 33 states and one territory, Puerto Rico. There is only one subcontracted organization per state, and each subcontracted entity was designated by the governor. Each state and territory identified a steering committee that is a private-public partnership composed of leaders from state government and stakeholder organizations, and all work is conducted through a series of coordinated work groups with specific charges. Each state or territory was expected to reach out to a broad range of stakeholders to include at a minimum:

- providers,
- payers,
- federal health facilities,
- state government,
- pharmacies,
- long-term care facilities and nursing homes,
- professional associations and societies,
- medical and public health schools that undertake research,
- hospitals,
- public health agencies,
- community clinics and health centers,
- laboratories,
- homecare and hospice facilities,
- correctional facilities,
- quality improvement organizations, and
- consumers or consumer organizations.

Methodology

The methodology developed for the project was based on 3 key assumptions. The first assumption is that, in order for stakeholders to trust electronic health information exchange, decisions about how to protect the privacy and security of health information should be made at the local community level. Second, to accomplish this goal, discussions must take place to develop an understanding of the current landscape and the variation that exists between organizations within each state and, ultimately, across states. Finally, stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the current variation, understanding the rationale that underlies the current business practices, deciding what the privacy and security requirements are, and developing solutions to achieve broad-based acceptance.

State teams followed a modified community-based research model that provided flexibility to each team to organize its leadership, steering committee, and work groups in ways appropriate to the needs of their current industry organization and market structure. Project teams followed a core methodology that framed discussions for the exchange of specific types of health information within 9 domains of privacy and security by using 18 scenarios as the starting point for work group discussions.

The 9 Domains of Privacy and Security

- User and Entity Authentication
- Authorization and Access Control
- Patient and Provider Identification
- Transmission Security
- Information Protection
- Information Audits
- Administrative and Physical Safeguards
- State Law
- Use and Disclosure Policy

All state teams were required to form a steering committee composed of state leaders and public and private stakeholders to provide leadership throughout the process and to sustain the effort beyond the end of the contract. Steering committee membership varied in accordance with the unique landscape and environment of each state and territory, but all committees were asked to include one member that represented the governor's office—either a senior policy advisor, cabinet member, or, in the case of one state, the lieutenant governor. The other members of the committees include high-level health care officials, such as directors of health insurance companies, health care, hospitals, and public health care systems.

Table ES-1 provides the number of stakeholders engaged during the assessment of variation process as reported by all 34 state teams. This table gives an idea of the scope of stakeholder input that has been incorporated into this work.

The general approach to the work consisted of 4 interrelated steps to conduct the Assessment of Variation. First, the Variations Working Group (VWG) members reviewed the 18 health information exchange (HIE) scenarios and generated a core set of business practices and policies consistent with the stakeholder roles represented in the scenarios. Project teams were then asked to categorize business practices as potential barriers to

Table ES-1. Number of Stakeholders Engaged in Assessment of Variations Process (All States Combined)

	Stakeholders Engaged in Variations Assessment through Community Outreach (Raw Numbers)	
Stakeholder Group	**(N)**	**(Avg.)**
Providers	1,630	48
Hospitals/health systems	341	10
Clinicians	240	7
Physicians and physicians groups	220	6
Community clinics and health centers	185	5
Professional associations and societies	157	5
Pharmacies/pharmacy benefit managers	85	3
Mental health and behavioral health	82	2
Long-term care facilities and nursing homes	74	2
Safety net providers	61	2
Homecare and hospice	44	1
Laboratories	43	1
Emergency medicine	42	1
Federal health facilities	37	1
Other health care providers	19	1
Technology and Health Information Experts	582	17
Privacy and security experts/compliance officers	141	4
Electronic health records experts	94	3
Health IT consultants	84	2
Quality improvement organizations	67	2
Technology organizations/vendors	58	2
Health information management organizations	56	2
Regional health information organizations	47	1
Other health data and technology experts	35	1
Consumers	458	13
Individual consumers	318	9
Consumer organizations and advocates	140	4
Other Government	243	7
Medicaid/other state government	193	6
County government	50	1
Public Health Agencies or Departments	213	6
Employers	198	6
Legal Counsel/Attorneys	181	5
Medical and Public Health Schools/Research	140	4
Payers	122	4
Law Enforcement and Correctional Facilities	37	1
Foundations/Other Policy Consultants	4	<1
Other	3	<1
Total	3,811	112

electronic health information exchange (eg, requirement for wet signatures); as potential enablers of or aids to electronic health information exchange; or as having no impact on the flow of information, whether on paper or electronically.

Second, the core set of business practices generated by the VWG was circulated to a broader group of stakeholders for validation and to generate additional business practices based on their experience. This step served to involve the broader stakeholder community, build consensus, fill gaps in the VWG membership, and check the accuracy of the practices generated by the VWG.

In the third step, the VWG reviewed the full set of collected business practices to ensure that the data were complete and sufficiently detailed for evaluation by the Legal Work Group (LWG); in addition, the VWG identified the policy driving the practice to better understand the rationale behind the practice(s).

Finally, the business practices that were flagged by the VWG were reviewed by the LWG to identify the legal drivers that might be relevant to better understanding the rationale behind the practice(s).

Current Nationwide Landscape for Privacy and Security Solutions

Analysis of the activity reported by the state teams reveals an emerging pattern that reflects the roadmap from paper-based health information exchange to full electronic health information exchange at the state level. The variation in the level of analysis, identification of solutions, and the scope and content of the implementation plans is driven by the current placement of the state on the road to statewide electronic health information exchange. One of the determining factors in the identification and selection of these priority solutions and implementation plans across states was the stage of development, adoption, and implementation of health information technology (HIT) and HIE initiatives within the state.

All state teams have some type of HIT/HIE activity currently under way, and these activities range from independent, isolated HIT efforts conducted by one health care organization (single organizations), to the implementation of one or more local or regional multiorganizational HIE efforts, to the early planning of a statewide electronic health information exchange effort, to the establishment of foundational components of a statewide initiative, to early implementation of a statewide HIE effort, to more mature, operating statewide implementations.

With respect to local or regional electronic health information exchange activity, all teams identified 1 or more such efforts currently under way within their states. Most of these efforts are set in defined geographic areas in the state, are funded through local, state, private, or federal funding, and involve 2 or more provider organizations. Some states have done extensive inventorying of both HIT projects and interorganization HIE initiatives. Ten

of the 34 state teams are currently considered to be in the early planning stages of statewide electronic health information exchange development. This stage includes states that have not yet identified or established an organization to facilitate the statewide planning process but do have an agency or government body conducting preliminary assessment of HIT/HIE efforts in the state. This stage also includes states that have an identified government body or entity responsible for developing a statewide plan. States in this group included Arkansas, Illinois, Iowa, Kansas, Mississippi, New Hampshire, New Jersey, Oklahoma, Oregon, and Puerto Rico.

Fifteen state teams have established some foundational components necessary for statewide electronic health information exchange development. These include states that have (1) identified and established a central body to coordinate HIE development; (2) appointed a governing body (board of directors); (3) established operating committees; and (4) completed a strategic plan or roadmap. States in this group included Alaska, Colorado, Connecticut, Kentucky, Louisiana, Michigan, Minnesota, New York, North Carolina, Ohio, Vermont, Washington, West Virginia, Wisconsin, and Wyoming.

Seven states were classified as having established early implementation, including Arizona, California, Florida, Maine, Massachusetts, New Mexico, and Rhode Island. In addition to the element identified in the previous stage of development, here the distinguishing factors were as follows: (1) some of the key roadmap implementation steps have been undertaken, (2) the statewide HIE initiative has selected a technology vendor, and (3) the state has begun implementing HIE pilots. In all cases in this group, the central coordinating body was a nonprofit entity.

This group was characterized by a fully functioning statewide HIE effort, albeit the effort may be supporting only 1 or just a few types of clinical electronic health information exchange (ie, clinical labs, medications, note documentation, billing, claims scrubbing). Only 2 states, Indiana and Utah, were considered to be at this stage of development.

Across the board, state government roles in the planning and implementation of statewide HIEs varied from active participation to being a co-lead facilitator, to serving as the lead convener and providing initial funding support for the planning process and, in some cases, funding the initial infrastructure investment needed to launch statewide HIEs.

For most states at a foundational level or early statewide implementation stage that have completed a statewide implementation plan, the financial plan called for a significant foundational support from state government, federal government, or both to launch the effort.

Assessment of Variation, Analysis of Solutions, and Implementation Planning

Section 6 in this report presents issues that state teams identified as critical and in need of resolution. First among those issues is the need to harmonize the approach to patient permission for disclosure.[2] Thirty of the 34 state project teams cited the need and process for obtaining patient permission to use and disclose personal health information as key to private and secure electronic health information exchange, and the area that requires the most work. Broad variation exists among organizational policies that determine when patient *consent* is required, how the *consent* is obtained and documented, and how patient permission is communicated to health care organizations, payers, and other outside entities. State teams suggested a wide range of solutions to address the differing definitions and applications of patient permission. One of the most frequently cited solutions was the creation of a common or uniform permission form for both paper and electronic environments. State teams proposed 3 general designs for permission documents: a uniform permission form used by all; a standardized permission form that includes certain elements, but may be modified based on institutional preferences; and models that would allow institutions to draft their own forms. Each option has positive and negative aspects, including the amount of work required to achieve consensus on the necessary elements and the complexity of managing those elements in an electronic system. Many state teams have indicated that they want to maintain the requirement for patient permission but make it more workable in an electronic environment, and they plan to fully catalogue state permission requirements (at least for treatment) and work to harmonize the permission process requirements.

Whatever solution the state teams identify must also accommodate federal laws that impose additional requirements on the exchange of certain types of health care information requiring patient permission for disclosure. The Family Education Rights and Privacy Act (FERPA) governs most school records; under FERPA's privacy and security regulations, information contained in a school health record is considered an education record (not *protected health information,* as HIPAA stipulates), which requires permission for disclosure, with the exception of health and safety emergencies (45 C.F.R. § 160.103; 34 C.F.R. § 99.31). The Clinical Laboratory Improvement Amendments (CLIA) were also cited for conflicts imposed on states because of ambiguous terms.

[2] The terms *consent* and *authorization* have specific meaning under various federal and state laws. For the purposes of this discussion we have adopted the neutral term *permission* to refer to the concept of obtaining written approval from a patient to use or release health information. The terms *consent* and *authorization* are used where appropriate (ie, in discussions of HIPAA's treatment, payment, and health care operations exceptions).

States also reported the need to incorporate requirements of federal laws governing the confidentiality of alcohol and drug abuse patient records and Medicaid information.[3] These topics are more fully discussed in Sections 6.2.4 and 6.5.

The state teams have made it clear that the interplay among the HIPAA Privacy and Security Rules, other federal laws that protect sensitive data, and state privacy laws creates a complex environment where what is required is not always clear. Some state teams have called for treating all health information as specially protected, which would raise the privacy bar but reduce the variation.

States reported many business practice variations based on different interpretations and applications of the requirements of the HIPAA Privacy Rule. Section 6.2 summarizes some examples from the state teams regarding HIPAA Privacy Rule issues that pose challenges to electronic health information exchange. State teams recommended 4 general categories of solutions to address the variation caused by differing applications of the Privacy Rule and state law: education programs; standard policies and practices; creation of a compendium of state law, federal law, case law, and preemption analysis; and requests for federal guidance. The acronym "HIPAA" has become a generic term for privacy and security practices, even though restrictions are often imposed by state law or practices resulting from misinterpretations of the HIPAA requirements. State teams planned to offer additional education for providers, perhaps as a continuing education requirement. The recommendation for education programs included suggestions for a variety of topics: addressing differences in state law and the HIPAA Privacy and Security Rules that pose challenges to electronic health information exchange; public misconceptions of the HIPAA Rules; specific areas of misunderstanding, such as use and disclosure of information to personal representatives; and definitions of terms as they apply to paper and electronic environments.

Standard policies and practices are another potential solution. State teams suggested creating policies that address routine exchanges of information both in regular and emergency circumstances. These exchange models would comply with both the HIPAA Privacy and Security Rules and state law. The policies and practices would have to be developed by the appropriate leadership body and be reviewed by a variety of stakeholders. Once developed, the body would disseminate the policies and offer educational programs to explain their significance and implementation strategy. This solution may prove useful in certain circumstances, but may be less feasible, given the wide range of circumstances and situations that organizations face. Alternatively, state teams suggested compiling relevant state law, federal law, case law, and preemption analyses. State privacy laws were generally passed over time and are frequently scattered throughout many chapters of the

[3] 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.

state code. Case law may also contain conflicting interpretations. State teams requested that the HHS Office for Civil Rights (OCR) publish de-identified case studies that describe the type of privacy lapses that are identified during enforcement activities and what corrective action was taken. It is important to note here that OCR now publishes specific but de-identified case examples of corrective action obtained from *covered entities* through enforcement of the Privacy Rule. Section 6.4 of this report discusses the variation in the interpretation and implementation of the HIPAA Security Rule, with state teams indicating that the majority of stakeholders were not familiar with appropriate security policies, procedures, and technical solutions. State teams found that legal standards for security are lacking at the state level and are generally perceived to be inadequate or vague. Sharing personal health information among institutions requires a significant degree of trust in the technology, and in the other organizations' ability to implement it. State teams found that much of the concern about security came from providers who were worried that entities receiving their data might not have security measures as robust as those of their own organization, and that they might be considered liable in case of a security breach. Related to this concern was a lack of understanding that security in health care is far more complex than just the adoption of appropriate technical standards. Thirty-one state teams offered technology-based solutions to security issues. The level of specificity in the solutions varied widely, from general statements that certain technical issues must be resolved to achieve an acceptable level of security to very specific and detailed discussions of how to resolve specific issues. For example, one report provided specific technology-based solutions to security issues encountered during the creation of an HIE program in their state, including user/entity authentication, access controls, patient and provider identification, protection of sensitive health information, protocols for information transmission, audits, and use and disclosure policies.

Specific state law and interstate issues are discussed in Section 6.5. The major source of variation in business practices and policies stems from each state's unique privacy and security laws. Some of these issues have roots in federal legislation, although the true source of variation often lies in the state statutes. A major reported source of variation, state law that applies to sensitive health information, is discussed in Section 6.2.4, which addresses the variation in permission requirements. Many of the proposed changes to state law are very specific and apply to a narrow range of circumstances in a single state. For example, one state has a burdensome law that requires extensive documentation of disclosures of information, even verbal communications, between medical staff treating a patient in a single facility. Identifying laws that create challenges to interoperability, understanding the reason that the law was passed in the first place, and determining potential solutions require a thorough legal analysis. State teams have carefully considered the implications of amending state laws and, in many instances, have created options for language that could be used to amend the relevant law, and have discussed the pros and cons of each choice, as well as the implications of leaving the law as is. These very specific

changes are not addressed in detail here, but the following are general areas in which state teams plan to amend state law:

- Update or create legal definitions of terms (ie, *medical record* or *record locator service*) to apply to electronic exchange.
- Amend state privacy laws that do not sensibly apply to electronic exchange to include protections for electronic data.
- Create enforcement mechanisms for any new privacy or security laws.
- Consolidate state law or compile a compendium of relevant state law, federal law, and case law to facilitate legal analyses.

State teams were careful to note that they wished to proceed cautiously in amending state law, observing that the change could have unintended consequences, such as inadvertently limiting exchange instead of facilitating it.

Trust continues to be a critical issue that affects the potential adoption and viability of electronic health information exchange. Section 6.6 discusses the concerns that consumers and providers expressed; it also outlines areas where underlying trust issues lead organizations to draft extremely conservative policies that contribute to the variation in business practice and policy. Consumer concerns focused on privacy risks arising from the implementation of new technologies and the potential for unauthorized disclosures of *specially protected health information* to payers and employers. Providers were principally concerned about potential liabilities arising from the activities of other participants in health information exchange and about consumers' lawsuits for inappropriate disclosures of their information; they were secondarily concerned about potential uses of patient information by payers, law enforcement, and public health officials. The latter concern had less to do with trust in the security of the EHRs themselves, and more to do with how these systems might manage the competing interests between groups about access to EHR data.

Trust emerged as a major underlying issue. In some cases, trust (or lack of it) seems to have been a motivating reason for the variance in business practices. In a number of cases, stakeholder groups (other than consumers) articulated their impression that consumer lack of trust was a critical issue, but the concerns were neither supported nor denied by consumer input. Ten of the reports lacked information that either expressly, or by reasonable inference, raised trust as a critical issue.

The ability to accurately identify patients across systems was an issue in many states: 16 state teams suggested technical solutions to this issue. For the most part, these state teams agreed that some system of identifying patients between entities must exist for true interoperability to occur, and that these systems must include stringent matching criteria to ensure that patient records remain confidential. A discussion of the importance of patient and provider identity matching is provided in Section 6.7. Many state teams reported other major challenges: the variability in methods across organizations to link patients to records,

and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational electronic health information exchange is conducted. These challenges were not the case in uniquely identifying *providers* across the health care system, because new federal HIPAA regulations have now established a national standard unique identifier for health care providers (the National Provider Identifier [NPI]). Providers, payers, and others are required to fully implement the NPI by May 23, 2007.

Given the lack of a national (or state) unique patient identifier, state teams discussed several alternatives for future use under organized regional networks, and aimed at addressing the need for matching patients to their records across systems. One frequently cited mechanism was the record locator service (RLS), a centrally administered function of a health information network that provides the requester of data with the location of data about a specific patient. The RLS uses various identifying characteristics of individuals to create a match and to identify the location of health information for that individual.

State teams referenced a number of cultural and business issues that pose challenges to electronic health information exchange; these issues are discussed in Section 6.8. One example is concern about liability for incidental or inappropriate disclosures, which causes many stakeholder organizations to take a conservative approach to developing practice and policy. This concern is discussed in greater detail in Section 6.3.6. General resistance to change is another business issue that organizations face whenever a change occurs in how business is conducted, which in turn, can cause workflow modifications. Some individuals within organizations are comfortable with existing paper-based or manual systems and data exchange practices and processes, and they believe that current manual practices produce accurate data and are timely and effective. Implicit in some discussions is an assumption that security slows down the process: the data are secure but are not transmitted as fast as they can be with a quick phone call. In fact, most data exchanges take place via person-to-person contact, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be critical to include these points at which human judgment is required in the specifications for any system developed to exchange information.

Recommendations for Future Directions

The goals for this project have been achieved. State teams assessed variation, developed solutions, and considered how to implement those solutions. Each team developed a body of knowledge that has been shared with stakeholders within each state, and many state teams have begun to move forward with their plans. Of necessity, each team worked within its own state environment in this first phase of the process; however, to reduce variation in practice, policy, and law to a manageable range for nationwide electronic health information exchange, state teams will need to work with one another and with existing federal initiatives. To reduce variation moving forward, a coordinated effort will be required so the

34 state teams can work with teams from the remaining 22 states and territories to resolve key issues and to ensure agreement on a manageable range of solutions that can be translated into the privacy and security requirements for nationwide health information exchange. State teams have prioritized their plans, based on the needs dictated by their unique local environment for electronic health information exchange. It will be important to cluster the state teams into collaborative work groups that will each work on a topic that is both a priority for each state or territory, but is also applicable to the other states and territories. Periodically, the collaborative work groups should come together to share their progress and get input from the broader nationwide collaborative.

The next goal is for the work of the collaborative work groups to be adopted nationwide. This model provides the central coordination necessary to ensure that the work reduces variation nationwide by allowing the stakeholders within each state to push the issues and recommendations up to the collaborative work group. The model also provides a mechanism for interaction with the appropriate federal initiatives. This process is naturally recursive, as new issues are raised and work groups evolve. In addition to the organization of the state teams moving forward in the short term, observations and recommendations based on the Nationwide Summary are provided in Section 7.