APPENDIX A
STATE SUMMARIES

APPENDIX A
STATE SUMMARIES

ALASKA—SUMMARY

Alaska health care leaders and members of the Alaska Telehealth Advisory Council formed the Alaska Regional Health Information Organization (RHIO) in December 2005 to improve health record exchanges, lower costs, and prevent medical mistakes. The Alaska RHIO began formulating "next steps" in the health information exchange (HIE) process for Alaska. A large gap quickly became apparent between the perceptions of security and privacy and the practices related to security and privacy.

The Alaska RHIO, with the support of the Alaska Governor's Office, successfully competed for a national contract to perform an assessment of security and privacy issues. The Health Information Security and Privacy Collaboration is part of a national effort to share patient health information among health care providers, insurers, and health care agencies. Participation in the national initiative gives a voice to Alaska-specific issues, needs, and recommendations in the development of national policies related to security, privacy, and best business practices surrounding interoperability of HIE.

The HISPC project coordinator organized a core state project team that included members from the State of Alaska, the Alaska Electronic Health Record Alliance, Alaska Native Tribal Health Consortium, health care consumers, and legal and meeting facilitation contractors. The core team and other statewide participants made up the Variations Work Group (VWG). This group developed a list of stakeholders who were invited to participate in a series of regional stakeholder meetings.

Four regional (Anchorage, Fairbanks, Juneau, and rural providers) stakeholder meetings were held to gather input on business practices currently in use around the state as related to the security and privacy of electronic health information exchange. Approximately 120 people participated in the stakeholder meetings, while others agreed to provide input on project draft documents via e-mail and through the project website.

Meeting participants were grouped by area of interest and work environment. The participants were asked to discuss scenarios provided by RTI International that dealt with health care issues relating to treatment, payment, RHIOs, research, law enforcement, prescription drug use/benefit, health care operations/marketing, bioterrorism, employee health, public health, and state government oversight. Participants were also asked to prioritize security and privacy issues that they felt were of utmost concern in HIE.

Issues identified during the scenario discussions were as follows:

- The Alaska constitution guarantees privacy to every citizen of Alaska. This guarantee may require an opt-in model for development of health information.

- Most medical records are still paper; therefore, the most common ways of sharing health information today are via mail, via fax, and verbally.
- Even if electronic records are available, the information is rarely shared electronically, because the information systems are not compatible.
- Medical information is often sent by unencrypted fax or e-mail.
- It is important that all stakeholders have a role in the development of, and policy setting for, security and privacy issues related to HIE. This role becomes even more important in the discussion of RHIOs and electronic health records.
- Some of the scenarios provided did not relate to the Alaska health care environment, either because the type of information sharing would not happen in Alaska because of the privacy guarantees provided in the Alaska constitution, or because the scenarios included the sharing of information with adjacent states (there are no states adjacent to Alaska).

After the statewide meetings, Ellen Ganley and Rebecca Madison of the core team drafted an Interim Assessment of Variations report. This report was widely distributed to participants from the original statewide meetings and to additional stakeholders throughout Alaska. The report was also reviewed by the core state project team, the VWG, the Legal Work Group (LWG), and the project steering committee. Input was collected via e-mail and web forums. The report was submitted to RTI on November 6, 2006. Numerous financial, legal, and logistical barriers to HIE were identified and categorized within the report.

After reviewing the Interim Assessment of Variations report, the core State team formed an Alaska Solutions Work Group (SWG) to address the issues raised in the variations report. The Alaska SWG contains a variety of participants in the health care system, reflecting a cross-section of the population very similar to that of the core team and the participants in the statewide workshops. The SWG was tasked with addressing each of the barriers identified in the variations report and determining if they were actually barriers and, if so, how solutions to the barriers could be addressed.

Assisting in this task was the Alaska LWG, which included lawyers in private, government, and nonprofit practice, who met in a series of weekly meetings to address the issues raised as legal barriers. The LWG identified several of the legal barriers able to be addressed through state or federal law exceptions that allow the practice to continue or the barrier to be overcome. For the issues that remained as barriers, the LWG attempted to determine whether they should be addressed by legal, legislative, or business practices. This information was passed on to the SWG to assist with the identification of solutions.

The key solutions identified were as follows:

- Legal solutions would
  - encourage legislative efforts to standardize Alaska laws regarding confidentiality and use Health Insurance Portability and Accountability Act (HIPAA) preemption analysis (currently in draft form only) to identify areas requiring standardization;
  - enact laws and regulations in support of HIE and electronic health records, including immunity or statutory limitation on liability for RHIOs; and
  - identify applicable legal exceptions and aids to providers and patients.
- Standardization of policies and procedures would include
  - identification standards including standard list of demographic information for patients;
  - standard authorization policies and procedures across all participant organizations;
  - standard policies, procedures, and training regarding confidentiality;
  - standard policies, procedures, and training regarding use and disclosure of health information, in accordance with HIPAA and state law, including use and disclosure by personal representatives or health care power of attorney;
  - standard policies and procedures regarding auditing and monitoring, including patients' access to monitor their own records; and
  - identification of proper access and permission levels for a variety of staff.
- Participant agreements would include
  - business associate agreements tailored to RHIO and HIE purposes, to be used only as necessary to limit liability;
  - education regarding proper use and application of business associate agreements;
  - determination of whether an opt-in system or opt-out system would be more successful and which system would be more efficient and cost-effective; and
  - drafting of standardized forms for use by all participating organizations and patients, forms including but not limited to authorization, HIPAA forms, disclosure logs, reports of unauthorized access, and patient requests for records.
- Education and marketing would include
  - statewide informational sessions for consumers to explain benefits of the system and answer questions regarding privacy and security;
  - education and training for providers regarding proper procedures, need for standardization, and benefits of HIE and RHIOs;
  - informational sessions tailored for legislators and government to raise support for HIE and RHIOs and for necessary legislative and departmental changes;

- marketing tailored to consumers and providers to encourage use and participation in HIE and RHIOs and to raise funds for ongoing operation of the system; and
- targeting of particular sources to raise funds for technology necessary for full participation by providers and patients.

ARIZONA—SUMMARY

Arizona Governor Janet Napolitano signed an executive order in 2005, initiating the development of the Arizona Health-e Connection Roadmap, making the electronic exchange of health information a priority for the State of Arizona. A steering committee composed of major stakeholders was convened to develop the Roadmap.

The committee was charged with identifying legal, technical, and clinical practices that relate to electronic health information exchange (HIE). A key issue that emerged related to security and privacy concerns that arise from the electronic transfer of health information between health care entities (see Arizona Health-e Connection Roadmap, http://www.azgita.gov/tech_news/2006/4_5_06.htm).

The Arizona Health Privacy Project (AHPP) was launched in June 2006 with the Health Information Security and Privacy Collaboration (HISPC) contract. This award was part of the US Department of Health and Human Services project, Privacy and Security Solutions for Interoperable Health Information Exchange. To lead this Arizona effort, a state project team consisting of representatives from the Government Information Technology Agency; the Arizona State University's Center for Advancing Business Through Information Technology; and the law firm of Coppersmith, Gordon, Schermer & Brockelman, PLC, was chosen.

As required by the HISPC contract, the AHPP first convened the Variations Work Group (VWG) to generate information on security and privacy business practices across Arizona. The VWG reviewed 18 factual scenarios prepared by RTI International (the HISPC prime contractor), which were designed to elicit information about security and privacy practices in HIE. Working concurrently with the VWG, a Legal Work Group (LWG) was convened to evaluate potential legal issues for e-Health data exchange in Arizona. As a result of the information-gathering and analysis process conducted by the VWG and the LWG, the groups identified several critical issues that create barriers to the electronic exchange of health information in Arizona.

The VWG and LWG findings related to the principal barriers to information exchange that are detailed in the state's report can be summarized as follows:

- Health care organizations in Arizona use different media to share critical information. These multiple communication methods pose challenges to response to information requests.

- Health care organizations interpret the Health Insurance Portability and Accountability Act regulations inconsistently and implement safeguards that may be either overly restrictive or lax. These differences in interpretation pose a barrier to e-Health data exchange.

- Health care organizations in Arizona face different financial constraints on whether or how much they invest in technologies such as encryption and secure e-mails to protect patient information.
- Arizona laws protecting genetic testing information, communicable disease information, mental health information, Arizona Health Care Cost Containment System member health information, and immunization may pose barriers to e-Health data exchange.

Following the work of the VWG and the LWG, a Solutions Work Group (SWG) was convened to focus on identifying, proposing, and developing workable solutions to the identified barriers for HIE. The SWG and LWG held two work group meetings and augmented these discussions with conference calls between meetings to discuss the critical barriers and possible solutions.

The list of potential solutions generated by the SWG and LWG fell into 9 categories, all of which are explored in the report:

- development of a regional HIE
- solutions for authorization and authentication problems
- solutions for secure information transformation and exchange
- solutions to prevent unauthorized modifications
- solutions for current paper-based systems
- enhancement of the patient's role in controlling his or her personal health information
- other solutions
- solutions affecting state law or regulations
- solutions affecting federal law or regulations

The next step is to convene an Implementation Work Group to create a plan to address the barriers identified by the SWG and LWG.

ARKANSAS—SUMMARY

Like many states, Arkansas is faced with crises in health and health care. Arkansas demonstrates high rates of diabetes, heart disease, and cancer. Many of these conditions result from behavior and lifestyle choices (eg, overeating, physical inactivity, consumption of tobacco products). The widespread expression of these diseases results in disproportionate utilization of services and increasingly burdens the health care system and impacts its ability to deliver quality care.

The health care culture would be positively changed by monitoring and documenting of the quality of care delivered and would be optimized by the development and implementation of an interoperable electronic health record (EHR). Use of EHRs has been shown to decrease costs, reduce medical errors, and improve access to care in systems in which they have been incorporated.

The opportunity from RTI International and the National Governors Association Center for Best Practices to participate in the Health Information Security and Privacy Collaborative (HISPC) allowed Arkansas to examine variations in laws and business practices related to privacy and security of health information exchange (HIE). Examination of variations in turn allowed Arkansas to determine potential solutions that would improve the status of electronic health information in the state through incorporation of interoperability standards and protocols. It is hoped that the Arkansas HISPC project will serve as a platform to facilitate ongoing efforts that will ultimately result in improved efficiencies of and access to care, decreased medical errors, enhanced continuity of care, and reduction in escalating health care costs.

In 2005 the Arkansas Center for Health Improvement (ACHI) was designated by the Arkansas Governor's Office as the HISPC project lead, which was to be in close partnership with the Arkansas Department of Health and Human Services (ADHHS) and the Arkansas Foundation for Medical Care (AFMC). These organizations already partner closely on a range of health-related projects, and their leaders regularly serve as advisors to policy makers in the state. In particular, ACHI and ADHHS have been instrumental in the success of the Healthy Arkansas initiative. AFMC leads a number of projects critical to advancing health information technology and also supports ADHHS by housing and analyzing data on Arkansas Medicaid recipients. The 3 organizations, with oversight and coordination by ACHI, were recognized as well positioned to organize stakeholders, examine challenges, and craft and implement pragmatic solutions intended to potentiate interoperability of HIE and, ultimately, improve the health of Arkansans.

In the initial request for funding, the Arkansas HISPC state project team set out a work plan and series of goals. With the submission of this report, all goals have been achieved in a timely manner, and the work plan is complete.

During the project period, the Arkansas HISPC stakeholder group was open to all those in Arkansas expressing interest. As a result of substantive recruitment efforts, membership of this group was both diverse and representative. The stakeholder group consisted of 125 interested parties from various health care communities, including hospitals, physician groups, clinics, pharmacies, payers, IT administrators, and others. In order to promote stakeholder group member retention and interest, the state project team utilized the webb portal made available by RTI. Stakeholder group members used the discussion forum to review the content regarding concurrence with or discrepancies identified in existing business practices. Members were also encouraged to use this tool to provide information on pertinent but *unidentified* business practices. Finally, all Arkansas HISPC work groups (Variations Work Group [VWG], Legal Work Group [LWG], Solutions Work Group [SWG], and Implementation Planning Work Group [IPWG]) were populated by members from the broader stakeholders' community.

During the course of the Arkansas HISPC project, the VWG held two meetings and identified more than 22 business practices impacting HIE in sites including but not limited to hospitals, community clinics and health centers, and pharmacies. Payer and consumer perspectives were also incorporated in the information assembled by the VWG. All 9 domains were impacted by the business practices identified as currently being used by Arkansas stakeholders.

The HISPC LWG was convened twice. The LWG served two distinct purposes, the first of which was to classify business practices identified by the VWG according to whether they acted as a barrier to HIE, were neutral to HIE, or functioned as an aid to HIE. After this initial classification, the LWG then identified what state or federal laws were implicated by those business practices. Nine business practices where designated by the LWG as barriers, 6 were designated as neutral, and 1 could not be assigned a distinct classification. Employing the legal expertise of the Brock-Chad Group and drawing upon the resources of its membership, the LWG was able to find specific state and federal laws that applied to most of the business practices. However, in some instances the LWG determined that supportive legal authority (authorizing, mandating, or prohibiting behavior) did not exist for certain practices.

The HISPC SWG held two meetings during the course of this project. The SWG was charged with developing recommendations to address the business practices identified as either barriers to HIE or neutral to HIE. The SWG examined each practice individually and, through an interactive brainstorming process, derived a series of potential solutions. The SWG then vetted and ranked these solutions on the basis of the state's ability to implement them.

The HISPC IPWG convened on 3 separate occasions to discuss the products derived serially and sequentially by the VWG, LWG, and SWG. The IPWG examined each recommended solution and crafted a series of implementation plans.

CALIFORNIA—SUMMARY

President George W. Bush issued an executive order on April 27, 2004, announcing his commitment to promote the use of health information technology to reduce medical errors, lower health care costs, and provide better information to consumers and physicians. The order called for widespread adoption of electronic health records and for health information to follow patients seamlessly and securely throughout their care. Similarly, Governor Arnold Schwarzenegger issued Exec. Order No. S-12-06 on July 25, 2006, to use HIT to improve patient safety and coordination of care, empower consumers, and guarantee timely access to care specialists. Most important, the governor's order highlighted his foundational pledge to identify and develop strategies to continue protection of the confidentiality and privacy of patients' health information for the purposes of health information exchange (HIE).

California's participation in the Health Information Security and Privacy Collaboration (HISPC) initiated diverse public and private health care industry involvement toward securing the privacy and confidentiality of personal information in HIE. Recognizing California's unique challenges due to its large population, geography, and industry, multiple stakeholders actively engaged in the 3 RTI International project phases of data collection, solutions analysis, and implementation plan development throughout the 8- month contract. The California state project team consisted of a public-private partnership between the California (State) Office of HIPAA Implementation and the California Regional Health Information Organization, which together managed the project. The team also included several nationally recognized legal, health, and technical experts, including Manatt, Phelps, and Phillips, LLP, the consulting firms of Object Health and Medical Management Services, and the RMA Consulting Group.

California is a recognized leader in the protection of personal health privacy. A strong commitment to patient privacy and the protection of health information is demonstrated in the state constitution and multiple statutes. However, state privacy law, often more stringent than the Health Insurance Portability and Accountability Act (HIPAA), has led to complex state and federal law interplay, often resulting in multiple and conflicting interpretations of applicable law. California stakeholders believe that such laws and corresponding business practices and policies are not barriers to HIE but instead represent California's commitment to strong individual-privacy protections. Moving forward, California's leaders recognize the foundational legal work that must be completed to create a new legal framework that will increase industry and public confidence in HIE.

The following summarizes the 5 major issues identified during the course of the RTI project.

Statewide privacy and security oversight body. The HISPC project established the first public-private infrastructure to address privacy and security issues. When potential solutions

to address business practice variations were analyzed, it became apparent that the time frame for the project did not allow for adequate research, analysis, and testing of privacy and security solution options. To adequately address the solution options beyond the project's time frame, an oversight infrastructure is required.

Operations. By applying only to "covered entities," HIPAA created a distinction concerning which Privacy and Security Rules apply to which members of the health care industry. In addition, stakeholders reported business practice variations stemming from disparate interpretations and understandings of HIPAA, state law, and their intersection. Lastly, stakeholders reported business practice variations that result from entities' selecting different approaches to implementing the optional and addressable provisions in HIPAA.

Technology. Because HIPAA created different security standards for different entities, permitting different approaches to HIPAA implementation, common security standards designed to protect health information have not been established that apply to all data exchanges as part of an HIE. Common data architectural standards[1] and detailed data classifications[2] have not been developed to differentiate between information required to support financial transactions and information required solely for treatment. Further distinction necessary within treatment data and within standards for auditing, authentication, access, and the like have yet to be reached.

Complexity of laws. California has many statutes governing the privacy and security of information, some of which were designed for different purposes and do not harmonize well. HIPAA preemption complicates the interpretation and understanding of the applicability of state laws pertaining to privacy and security. As a result, entities base business practice policies on a variety of interpretations that direct the access, use, and disclosure of medical information. Widespread variation in interpretations was particularly evident among communities less experienced with collaboration and information exchange. Additional problems arise when health information is exchanged across state lines, as the number of applicable statutes and variations in legal interpretations compound.

Trust. California stakeholders concluded that there are certain situations in which dynamic tensions may arise between patient privacy and necessary disclosures of medical information. One factor that stakeholders believed inhibits development of HIE privacy and security standards is the "tension" that results from the conflict between a patient's right to privacy and a provider's responsibilities to disclose health care information for payment and health care operations activities. All stakeholders agreed that health information should be exchanged for treatment; however, there appeared to be a belief that the release for payment or health care operations would not be limited to the information or purpose stated

[1] *Data architecture* is the method by which medical records are organized to ensure that the appropriate data is accessed for the appropriate purpose and only by the authorized entity.
[2] *Data Classification* is the content of the folders that contain medical records, such as a folder that may contain sensitive information accessible to limited entities for limited purposes.

for the disclosure, especially given the amount of information available through HIE. This issue should be resolved early on to prevent any further erosion of trust between consumers and providers.

COLORADO—SUMMARY

Colorado's statewide health information exchange (HIE) initiative is linking together diverse health care providers and platforms with a state-level, nonprofit oversight and operations entity, or hub, the Colorado Regional Health Information Organization (CORHIO). CORHIO leads development and will provide centralized operations for a federated interoperable HIE serving all of Colorado. Colorado is one of 6 state and regional demonstration (SRD) projects funded through contracts with the Agency for Healthcare Research and Quality. The SRD project—named the Colorado Health Information Exchange—provides technical expertise for development of the prototype point-of-care clinical data exchange that will become one of several types of HIE services supported by CORHIO. Other HIE types will include clinical and administrative messaging and population data exchange.

The privacy and security project's scope of work and methodology is built upon the structure, processes, timing, and significance of Colorado's HIE initiative and SRD project. CORHIO as a formal organization was recently incorporated and is on track to begin production-lab data exchange to meet terms of its AHRQ contract in fall 2007. The solutions outlined in the state report, as well as the project implementation plan to be reported subsequently, are key to successful implementation of Colorado's federated HIE network and state-level RHIO.

The first phase of the privacy and security project involved analyzing business practices and policies currently used by various Colorado stakeholders to protect health information. An additional task was to compile an inventory and analyze state and federal laws and regulations that relate to HIE. This analysis revealed numerous variations in organizational practices, as well as possible statutory and regulatory barriers to the successful implementation of a secure, federated interoperable environment.

Particular aspects of privacy and security HIE architecture were prioritized for attention and solutions development. Across these areas, solutions were categorized according to how and at what level they would be addressed in the context of single-state-level, multistate-level, and national-level interventions. Categories included the following.

Governance-related. These solutions are imbedded within CORHIO policies that establish conditions of participation for entities seeking to exchange information via the interoperable network.

Business arrangements. These solutions are specified as part of business practices and agreements between CORHIO and participating entities (including those individual entities and organizations that comprise a participating entity's network of business partners).

Technical. These solutions require technical design and implementation for CORHIO and participating entities.

Guidance/education. These solutions involve technical assistance materials; they also involve activities, including education and training, that promote implementation of agreed-upon policies and practices and that clarify legal and regulatory requirements.

Public policy development. These solutions require revisions to state laws and regulations, federal laws and regulations, or both.

In summary, priorities for state-level solutions include the following:

- authentication methods, including standard information exchange agreements with an annual authentication protocol certification program, agreed-upon guidelines on authentication rules and protocols, password and role-based access, a federated authentication system, and unique digital user/entity/machine identifiers;

- patient identification, including minimum data required and optional data elements to be used to match and de-duplicate patients, including the criteria for transmission of such data, matching (what qualifies as a match, when human intervention is required) use of a master patient index, robust auditing mechanisms, and feedback mechanisms to entities regarding potential duplicates (which will involve establishing a threshold level of error for patient matching and defining the limits for specificity [false positives] and sensitivity [false negatives]);

- access and disclosure of sensitive health information, including mental health protected health information (PHI), drug and alcohol treatment, HIV/AIDS, genetic testing, and other sensitive conditions, consistent with federal and state requirements, to support improvements to data-sharing agreements and organization policies and procedures, including filters for data considered sensitive (by CORHIO policies), in order to suppress viewing by end users;

- methods to ensure secure PHI transmission (including encryption and others);

- methods to accommodate lower levels of interoperability (such as faxes and paper communications);

- methods to prevent modification of PHI during or after transmission and to verify original content (data quality, nonrepudiation, etc);

- guidelines for audit controls and proactive monitoring of system access, including audit schedules, as well as definition, identification and actions on inappropriate access/security breaches, audit logs, and record retention standards;

- policies and procedures related to the re-release of PHI originally received from a different data source;

- standard procedures and processes by which patients might make amendments to their health information;

- procedures to handle health information of decedents;

- methods for allowing consumer-patients to make opt-in, as opposed to opt-out, decisions regarding information sharing via a regional HIE; and

- determinations of what constitutes the legal record, legal liability issues within interoperable environments, handling of sensitive health information, ability to legally use a "global" authorization form, legal treatment of a RHIO under the Health Insurance Portability and Accountability Act, the role of a RHIO as a business associate, and liability issues between RHIOs and participating health care entities.

CONNECTICUT—SUMMARY

The Connecticut Health Information Security & Privacy Initiative is a collaborative project designed to assess how Connecticut's privacy and security business practices and policies influence the exchange of electronic health information. This initiative was a 3-phase project that defined the current health information security and privacy environment in Connecticut, assessed variations across business entities, identified barriers to legitimate flow of electronic health information, proposed solutions, and developed a proposed plan of action.

Connecticut's report, the final Assessment of Variation and Analysis of Solutions, is the culmination of 11 months of information collected through collaboration with both public and private stakeholders to assess the variation of health information exchange (HIE) business practices in Connecticut, as well as the development of solutions to the identified barriers. The state project team prioritized the 18 specified RTI International scenarios, which were used to facilitate work group discussions.

The following HIE barriers that had a current or potential impact in Connecticut were identified through work group discussions:

- *identity:* the lack of provider and patient identity management;
- *authentication:* the lack of trust mechanisms in digital transactions;
- *authorization:* the misinterpretation of the Health Insurance Portability and Accountability Act, lack of uniform authorization to release protected health information, and an inability to verify digital authorization across enterprises;
- *access control:* the lack of uniformity among local access-control decisions;
- *physical security:* the lack of standards for sharing de-identified data;
- *exchange protocols and standards:* the lack of guidelines for secondary uses of data, inconsistent definition of *minimum necessary*, lack of standards for interoperability, and inconsistent information exchange policies;
- *data integrity/authentication:* the lack of trust mechanisms for accuracy of data;
- *audit, digital signature:* the inconsistent policies governing privacy breaches of personal health information;
- *corporate policies and practices:* the longitudinal view not available and the current paper culture; and
- *state and federal laws, regulations, and practices:* the legal status of regional health information organizations (RHIOs), current federal laws, and current state laws.

The solutions proposed in the state report focus primarily on patient care scenarios, as well as on variations discussed during the bioterrorism and public health scenarios. The process used by the state team to identify and propose solutions included the following: defining local use-cases; identifying applicable national and international privacy and security standards; defining information privacy and security solution architecture; defining a visionary work flow; convening stakeholders to define possible solutions based on standards; convening the Solutions Work Group to refine possible solutions; convening the Legal Work Group to evaluate solutions; engaging eHealth Connecticut (Connecticut's acting RHIO) stakeholders to evaluate the feasibility of and prioritize identified solutions; and organizing and presenting final proposed solutions.

The organizational-level solutions include the following:

- adopting and deploying statewide security architecture, standards, and policies;
- authorizing HIE business associate agreements (BAAs) and enforcing uniform policies and procedures;
- deploying edge system;
- deploying organizational-level staff digital identities; and
- publishing patient and record locator indexes to community and statewide HIE agents.

The cross-organizational community and statewide solutions include the following:

- developing a cost justification analysis and secure funding for HIE (RHIO);
- adopting information security architecture;
- adopting statewide HIE standards/protocols to define uniform cross-enterprise digital documents/content to represent *routine health care exchanges*;
- adopting statewide HIE standards/protocols to define uniform cross-enterprise digital documents/content for *noncare exchanges*;
- adopting technical statewide HIE standards/protocols to represent provider and health professional workforce authorization permissions and credentials;
- adopting HIE standards to enable a uniform pseudonymization process;
- establishing uniform RHIO-wide information exchange policies and business agreements, including but not limited to BAAs;
- deploying HIE building blocks, including a patient identity cross-referencing service, a health record locator registry, transitional central fax services, data integrity/authentication/digital signature services, and audit services;
- creating a uniform digital patient-consent/authorization-to-release process;

- developing a consumer and provider educational campaign; and
- enrolling individual providers/entities and support deployment.

The federal and state laws/regulations solutions include the following:

- pursuing legislation to authorize HIE (RHIO) roles, accountability, and functionality;
- modifying state laws and regulations to facilitate the exchange of information for the continuity of patient care, including state agency participation;
- establishing a Digital Identity Management and Authentication Service for the health care workforce (one tied to facility and practitioner licensures), as well as corporate workforce identity solutions;
- establishing licensure-based providers with digital identity services; and
- funding HIE and providing a broad range of financial incentives.

The interstate solutions include the following:

- engaging cross-state HIE exchanges with Rhode Island, Massachusetts, New York, and Puerto Rico (because of Connecticut's sizeable Puerto Rican community);
- vetting common cross-state solutions through the National Governors Association Center for Best Practices State Alliance for e-Health; and
- developing model state laws, utilizing the National Conference of Commissioners on Uniform State Laws process.

The national-level solutions include the following:

- funding the deployment of HIE infrastructure and federal share of operational expenses;
- requiring government programs (eg, Medicare, Medicaid, Veterans Administration, the Centers for Disease Control and Prevention) to participate and support HIE solutions; and
- using the federal bridge to register, enroll, and integrate cross-state digital identity services.

FLORIDA—SUMMARY

Project Background

Florida's Agency for Health Care Administration (Agency) was awarded a contract by RTI International to participate in the Health Information Security and Privacy Collaboration. This project is part of a national effort managed by the US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology; the Agency for Healthcare Research and Quality; and the National Governors Association. Florida was one of 34 states and US territories responsible for managing the collection and analysis of data from the state's health care stakeholders on the variations in organizational business practices, policies, and laws related to the private and secure exchange of health information.

The Agency assembled a state project team that was knowledgeable about issues related to health information exchange (HIE) and that has experience in the business and legal areas of health information privacy and security practices. The state team took the lead on organizing core groups of health care stakeholders into work groups. These groups participated in facilitated meetings aimed at collecting data on how policies and laws related to HIE are applied in various situations across a variety of health care environments. The Variations Work Group (VWG) was given the task of reviewing health care exchange scenarios and identifying business practices related to each scenario. This group collected 168 responses to 22 scenarios representing approximately 47[3] different business practices.

The Legal Work Group (LWG) took each of the business practices that had been identified as a barrier to HIE and determined the legal challenges related to each barrier. The LWG found that the barriers were a result of inconsistent state and federal laws, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice. The data collection from these expert focus groups was used to create a series of reports, including an Interim Assessment of Variation report (Deliverable 2) and the Interim Analysis of Solutions report (Deliverable 3). Copies of these reports are available at http://ahca.myflorida.com/dhit/Privacy_ss.shtml.

Purpose of Report

The purpose of the final Assessment of Variation and Analysis of Solutions report is to illustrate the variations in organizational-level business practices, policies, and laws[4] related to the private and secure exchange of health information. This final report includes an

[3]The estimated number 47 is based on the total number of discrete business practices presented in theory, not necessarily on nomenclature.

[4]The term *law* used here refers to relevant regulation, statute, or case that is the primary underlying driver behind a business practice.

assessment of the variation in business practices, policies, and laws and an analysis of the solutions to the barriers caused by the variation. The report contains 8 main sections. Section 1 describes the background and purpose of the report. Section 2 is a description of the methodology used to collect and analyze the data presented, and a breakdown and analysis of each of the scenarios presented by RTI, including a description of the stakeholders' response to the scenario, the applicable domains, and the general observations of variations in practice and law. Section 3 summarizes the key findings from the assessment of variation. Section 4 includes an introduction to the analysis of solutions and describes the process of identifying and selecting solutions. Section 5 is an analysis of the state-level solutions, which is followed by a listing of the solutions that serve as national recommendations (Section 6). Section 7 summarizes the entire report and identifies next steps pertaining to the implementation of the proposed solutions. The appendix (Section 8) includes the analysis of the 4 Florida scenarios added by Florida's privacy and security team and a listing of the work group members.

Notable Observations

There were variations within and across stakeholder groups, variations related to the way privacy and security policies were applied to actual business practices as outlined in this report. Some of the variations resulted in barriers to HIE, such as inconsistent state and federal laws that resulted in variations in policy, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice.

A legal barrier to HIE is a statutory or regulatory requirement that prevents the free flow of health information. In order to maintain the confidentiality of personal health information and thereby maintain consumer confidence in the health care system, legal barriers to HIE are a necessity. However, many of the laws regulating HIE were created prior to the advent of electronic HIE. Consequently, many such laws are narrowly focused and often prevent or delay, perhaps inadvertently, the free flow of HIE to those who would otherwise be authorized to access the health information. These delays are especially problematic if they prevent timely access to health care, subject people to the stress and hazards of unnecessary tests, and, in general, negatively impact people's health and well-being.

The solutions outlined in the report address the variations within and across stakeholder groups, variations related to the application of privacy and security policies and laws. Based on the types of barriers identified by the VWG and LWG, the Solutions Work Group identified solutions that address laws and regulations to facilitate HIE; technical issues related to the secure exchange of electronic health information; administrative or organizational barriers to exchanging health information; and the need for more education and greater public awareness of the rules and laws that address HIE.

ILLINOIS—SUMMARY

The Health Information Security and Privacy Collaboration (HISPC) was formed by contract between RTI International and 34 other states, including Illinois. The goal of HISPC was to assess and provide solutions that address variations in organizational-level policies and state laws that affect privacy and security practices, including those related to the Health Insurance Portability and Accountability Act (HIPAA), and that may pose challenges to the interoperability of health information exchange (HIE). The prevailing principle behind HISPC is that workable privacy and security approaches and business practices are imperative for comprehensive information exchange solutions to facilitate quality improvement, medical error reduction, timely surveillance, rigorous research, and improved efficiency and affordability of health care.

The Illinois Foundation for Quality Health Care was designated by the governor of Illinois as the coordinating entity for the HISPC project. The Illinois HISPC steering committee (HSC) was the reporting body for Illinois' contract with RTI. In addition, the HSC received oversight from the Illinois Electronic Health Records (EHR) Taskforce, which was created by the Illinois General Assembly in 2005 to make recommendations on statewide EHR activity. As part of their charge, the HSC provided RTI and the EHR task force with the following:

- a comprehensive review of the privacy and security laws and business practices that pose a challenge to the proliferation of HIE within the state;
- a review of and examples of best practices and solutions within the state, in order to maintain privacy and security protections while encouraging interoperable HIE;
- recommendations to improve both organizational privacy and security business practices, and privacy and security state laws that currently adversely affect interoperable HIE; and
- a plan to implement the subcommittee's recommendations.

The HSC had under its purview several work groups to support its objectives. These work groups included a business Variations Work Group (VWG), a Legal Work Group, a Solutions Work Group (SWG), and an Implementation Plan Work Group (IPWG). The HSC determined the membership of the Work groups and reviewed and approved all work products resulting from the groups.

Business practices surrounding privacy and security of health information conducted by organizations in the state were captured and assessed by the VWG. Over 100 unique business practices among 30 representative organizations were discovered. The VWG determined that the uses of technology to capture, maintain, and share patient information vary tremendously among Illinois' organizations. As would be expected, business practices

surrounding privacy and security of health information were discovered to vary according to the level of technology available to an organization. However, several common themes appeared, regardless of the level of technology available to an organization. The varying array of interpretation and sometimes misinterpretation of HIPAA was a common issue, sometimes even within the same organization. Also, for paper-based organizations, sharing of information was shown to be based significantly on established, trusted relationships. The level and method of sharing was revealed to be based more on familiarity between the existing parties than on established business agreements; therefore, a telephone call from a trusted person would garner the requisite information and perhaps more than required.

One of the key findings of this study of business variations is that Illinois has very strong protections to ensure that privacy and security are maintained during the exchange of health information. There are extensive laws that apply to Illinois providers, payers, and others, establishing rights and obligations with respect to maintaining patient privacy and with respect to confidentiality and security of patient health information. These laws drive HIE practices in Illinois and should be taken into account in discussions on necessary information technology parameters and requirements for national electronic HIE. However, because there is currently little electronic exchange of information between organizations, there are few operational examples of these protections as they relate to electronic HIE.

Silos of technology utilization were found throughout Illinois. Many health care organizations have been able to incorporate significant technological resources to maintain patient data. This finding is particularly true of the major urban health care facilities in the Chicago area. However, little effort has gone into enabling organizations to share data electronically with one another. The most salient reason for this lack is that the culture in Illinois has not been conducive to data sharing. Information often has been deemed as proprietary and a business asset, as opposed to being deemed an opportunity to improve quality of care and patient safety. Although there is evidence that this trend is shifting, the shift is occurring slowly and sporadically. The cultural change and technical infrastructure necessary for sharing information will need to come together before the policies and procedures necessary to facilitate HIE begin to become more commonplace.

Critical barriers to the implementation of interoperable electronic HIE were elucidated further by the work of the SWG. Barriers were confirmed to exist in organizational culture, in technology and standards, in lack of knowledge at both the staff and consumer levels, in organizational resources for health information technology (HIT), in leadership for privacy and security protection, in the global market, and in relation to state or federal law, primarily in misinterpretations and noncompliance. Root causes for these barriers were determined to include needs for proof of the benefits of regional HIE, development of technical and professional standards, consumer and staff education, inclusion of economically disadvantaged providers, quality assurance in HIT, and clear and concise legislation and enforcement thereof. The SWG developed solutions to address these specific

needs and systematically prioritized them according to the maximization of patient care and outcomes, the feasibility of implementation, the maximization of privacy and security protection, the cost-effectiveness, the alignment with other state and national activities, and a reduced dependency on the accomplishment of other activities. The prioritized solutions forwarded on to the IPWG for implementation planning included the following recommendations:

- Determine benchmarks for regional exchange of information—perhaps by committee of industry (HIT and administrative) stakeholders, much as was done for HIPAA transactions.
- Adopt universal standards for patient identification by all accrediting agencies, with official, verifiable means of identification defined, with both primary and secondary identification factors required.
- Define professional qualifications for privacy and security officers.
- Establish core competencies for staff education.
- Develop educational materials for consumers for providers to distribute.
- Extend and promote, in discussion with the state's attorney general, national Stark and anti-kickback relief regulations, so those who are advantaged can support those who are disadvantaged.
- Provide recommendations for multidisciplinary teams for acquisition of new IT solutions.
- Include in lead state agency an organizational legal staff with expertise in privacy and security to guide integrated state efforts.

INDIANA—SUMMARY

Indiana, as one of 34 states and territories to participate in the Health Information Security and Privacy Collaboration (HISPC), assessed current business practices and Indiana state laws that affect health information exchange (HIE). The assessment was based on the scenarios provided by RTI International, identified barriers revealed from those scenarios, and developed proposed solutions.

Current HIE landscape in Indiana. Indiana has many advanced systems for the exchange of clinical information for the treatment of patients and other authorized uses, and it has distinguished itself as a national leader in the HIE field. There are multiple regional health information organizations in various stages of development. Additionally, although several Indiana health care stakeholders operate sophisticated electronic health record (EHR) systems, a good number of Indiana providers still rely on paper records or some combination of paper and EHR.

Variations process. The Indiana HISPC state project team gained the participation of more than 40 individuals and organizations from across the state for the Variations Work Group (VWG) assessment of the current business practice of Indiana stakeholders, basing this assessment on discussion of the 18 scenarios provided by RTI. The state project team was able to secure the involvement of all stakeholder types except correctional facilities and consumers (despite efforts to do so). The state project team identified and logged more than 166 business practices related to the RTI scenarios.

Barriers and solutions. Overall, Indiana law is favorable to HIE and imposes few restrictions, relying instead on the Health Insurance Portability and Accountability Act; however, some problem areas were revealed during the scenario review process. The barriers are summarized below and are listed in priority order, along with the proposed solution.

There are several other barriers to HIE that are not privacy and security related, such as funding and financial sustainability issues. However, these issues are outside the scope of this project.

Barrier	Solution
Federal Law: Drug and alcohol abuse treatment data are prohibited by 42 C.F.R. pt. 2 from being exchanged without consent, with consenting requirements being unclear. The way data is collected at mixed-use facilities also poses problems.	▪ Amend 42 C.F.R. pt. 2 to provide that patient consent is not required to exchange the data for treatment purposes. ▪ As an alternative, explore Health and Human Services's authority to define the contours of consent.
Business Practice: Misunderstanding of mental health record consent law. Indiana law does not require consent for disclosure of mental health records	▪ Develop a communication program to educate mental health providers that consent is not necessary.
Business Practice: Misunderstanding of communicable disease consent law. Indiana law does not appear to require consent for disclosure of HIV/AIDS or other communicable disease data.	▪ Develop a communication program to educate providers that HIV/AIDS is not treated differently than other communicable disease data and that consent is not required. ▪ Could also amend Indiana law to make it clearer.
Ambiguity in State Law: Ambiguity in pharmacist laws on sharing medication history data. Indiana law permits sharing of pharmacist's data only when it is in the "best interest of the patient."	▪ Amend Indiana law to regulate pharmacists' data under general medical records law, thus eliminating consent requirement.
State Law: Health Maintenance Organization (HMO) state law does not allow for sharing clinical data for research (eg, de-identified research) without patient consent.	▪ Amend Indiana law to permit HMOs to share health data for research purposes without consent, so long as HIPAA is followed. ▪ As an alternative, work with HMOs and employer groups to help them understand the benefits of use of data for research, and encourage them to include patient consent for HIPAA-compliant research in their plan documents.

IOWA—SUMMARY

Overview

Iowa was one of 34 states selected for the Health Information Security and Privacy Collaboration (HISPC) project during 2006–2007 through funding from the Agency for Health Care Research and Quality (AHRQ) and the US Department of Health, Office of the National Coordinator for Health Information Technology (ONC). RTI International and the National Governors Association provided overall project management. The project focus was *privacy* and *security* issues related to electronic health information exchange (eHIE). These efforts align with the president's ongoing goal to expand the use of health information technology (HIT) in the United States to lower health care costs and improve quality. Privacy and security issues must be addressed in order for HIT and eHIE to advance successfully.

Participating HISPC states were asked to

- identify variations in privacy and security business practices, laws, and regulations affecting the electronic exchange of health care data;
- determine if the practices, laws, and regulations pose a challenge or barrier to health information exchange;
- develop best practices and proposed solutions to address identified challenges; and
- develop implementation plans for the proposed solutions.

Findings from all participating states will ultimately be compiled by RTI in an overall HISPC "roll-up" report for submission to AHRQ and ONC.

Project Leadership

The Iowa project was led by the Iowa Foundation for Medical Care (IFMC) as designated by the Governor's Office. A project steering committee and 5 work groups composed of key stakeholders contributed to all phases of project completion.

Iowa HISPC leadership structure was as follows:

- Iowa HISPC steering committee
- Project staff: IFMC
- Variations Work Group
- Legal Work Group
- Solutions/Implementation Work Group: Operations

- Solutions/Implementation Work Group: Legal
- Consumer Focus Work Group

Project Phases/Deliverables

The HISPC project phases were tied to a series of deliverables. This report was the final Assessment of Variation and Analysis of Solutions (Deliverable 5) as shown in the table below.

HISPC Deliverable	Submission Date
1. Work Plan	June 9, 2006
2. Interim Assessment of Variation	November 6, 2006
3. Interim Analysis of Solutions	January 15, 2007
4. Interim Implementation Plans	February 14, 2007
5. Assessment of Variation/Analysis of Solutions	March 30, 2007
6. Implementation Plans	Due April 15, 2007

This report combines the content of Iowa's Interim Assessment of Variation and Interim Analysis of Solutions reports, but it further refines and expands on the interim findings. Copies of all Iowa HISPC reports are available from IFMC (e-mail: sbrown@ifmc.org).

Main Findings: Variations

The project revealed a wide range of practice variation and privacy and security barriers to eHIE in Iowa. The barriers were grouped into 5 main areas:

1. *operational:* barriers that result from variations in business policies and practices and are related more to operational decisions by organizations than to legal requirements.

2. *legal:* barriers that result from legal requirements; these may exceed the Health Insurance Portability and Accountability Act regulations, may be complex or confusing to providers, may be overly restrictive, or may vary by state.

3. *technological:* barriers that result from limitations in the technology features that protect privacy and security of eHIE; or technology features that actually impede efficient eHIE.

4. *consumer-related:* barriers that result from consumer perceptions about privacy and security of eHIE.

5. *provider-related:* barriers that result from provider perceptions and the cultural rural aspects of the State of Iowa.

Main Findings: Solutions

The barrier framework was used to begin development of privacy and security solutions for eHIE in Iowa. Given the limited project time frame, Iowa work groups focused primarily on operational and legal matters, with the intent that these would address many provider and consumer concerns, as well. Solutions not fully addressed during the project will be carried forward as a continuation of HISPC work. All viable solution ideas were documented for future reference.

Privacy and security solutions to facilitate eHIE in Iowa were as follows:

- *operational and Legal:* more fully developed ideas, with other ideas noted; and
- *technological, Consumer-related, Provider-related:* mainly noted but not developed.

Examples of proposed solutions included the following:

- formally coordinating existing Iowa HIT/eHIE initiatives;
- developing consensus documents and policies related to eHIE in Iowa;
- conducting eHIE educational efforts for providers and consumers;
- updating and consolidating Iowa laws related to medical record confidentiality;
- endorsing technological and security standards for eHIE in the Iowa health care community; and
- piloting a voluntary, community-based health information exchange.

The remainder of the report provides detailed methodologies and findings related to Iowa HISPC variations, barriers, and solutions. Iowa's implementation plans will be provided in the final Implementation Plans report (Deliverable 6). That report will also include further details on the overall strategy for continuing Iowa HISPC work after the project contract concludes.

KANSAS—SUMMARY

In most of the United States, citizens' and businesses' readiness to electronically exchange clinical information is nonexistent. The business case for such a capability continues to be debated. Technology standards are still too numerous to be considered stable. Privacy concerns remain incompletely addressed. And there is widespread uncertainty about the legal requirements surrounding disclosures of such data. Nevertheless, a substantial portion of the industry and the general population believe that electronic exchange of health data is something worth doing.

Kansas, like most states, is host to a handful of organizations making fledgling attempts to develop local or regional health information exchanges (HIEs). The state itself has sponsored a number of initiatives to help promote these activities. Nevertheless, Kansas, like most other states, has not yet produced a viable, generalizable HIE process. The broad lack of transformation to electronic means of exchange offers an opportunity, however. Kansas stakeholders are (1) keen to begin the process, (2) seeking best practices that will not be outdated in the midterm, and (3) unencumbered with legacy systems that would color their views or would have to be replaced by a future statewide approach.

The Health Insurance Security and Privacy Collaboration (HISPC) project was oriented around discussions of 18 hypothetical scenarios that would precipitate the exchange of protected health information. For each scenario, 9 "domains" (or "design dimensions") were considered, including 7 technical dimensions and two legal dimensions. Through participation in the HISPC Variations Work Group and the Solutions Work Group, a core set of more than 30 Kansas stakeholders (joined by an equal number on a less regular basis) engaged in these discussions. The stakeholder collaborations themselves are understood to be primary products of the HISPC process, and these collaborations are expected to outlive the project itself.

Plans for implementation of solutions generated by the Kansas HISPC discussions are under development. On February 7, 2007, Governor Kathleen Sebelius announced formation of the Kansas Health Information Exchange Commission. This group will be tasked with expanding on the work and implementing the recommendations of previous initiatives to promote the electronic exchange of health information while assuring its privacy and security.

Kansas stakeholders identified hundreds of variations in business practices that were seen as potential impediments to the adoption of health information technology. These tactical issues were reorganized by the Solutions Work Group into 4 strategic areas: patients, business operations, legal issues, and regional issues. The Kansas state team believes that successful solutions will be those that gain consumer acceptance and create market demand for new information products and services. It intends to encourage Kansas stakeholders to

continue to invent modest local and regional "pilot" solutions. By empowering these pilot solutions and initiatives, the state team hopes to foster better understanding of their feasibility, share lessons learned, and extend successes.

One benefit of HISPC will be the establishment of a strategic framework for conducting these demonstration projects, for sharing lessons learned, and for producing one or more interoperable models for HIE. In this way, it is hoped that some risks in investment and promoting growth of HIE best practices will be mitigated.

KENTUCKY—SUMMARY

Health care is the only industry of its size still dominated by paper, phone, fax, and mail. Most American clinicians still rely on file folders with handwritten notes, paper prescriptions, and incomplete patient histories stored in file cabinets. While patients and physicians benefit from sophisticated technology to diagnose and treat disease, the relatively basic information technology necessary to record, store, share, and protect health information electronically remains the exception and not the rule.

In Kentucky, rising health care costs; concerns over access to quality, affordable care; and poor health outcomes led a bipartisan group of leaders in the General Assembly and officials in Governor Fletcher's administration to work together on e-Health as a solution.

On March 8, 2005, Governor Fletcher signed Kentucky's landmark e-Health legislation, known as Senate Bill 2 (SB2), which authorizes the creation of a secure, interoperable statewide electronic health network. SB2 also created the Kentucky e-Health Network Board to oversee e-Health efforts in the state. Led by clinical leaders from Kentucky's two major research universities—the University of Louisville (U of L) and University of Kentucky (UK)—the e-Health board consists of a number of public- and private-sector health leaders and is attached to the Cabinet for Health and Family Services (CHFS).

Kentucky e-Health Privacy and Security Collaboration

One of the first projects undertaken by the e-Health board was the Kentucky e-Health Privacy and Security Collaboration. In May 2006, Kentucky was one of 33 states awarded a contract to participate in the Health Information Security and Privacy Collaboration, a federally funded collaboration involving the Office of the National Coordinator, the Agency for Healthcare Research and Quality, RTI International, and the National Governors Association. Governor Ernie Fletcher designated CHFS as the project manager but requested that CHFS staff work collaboratively with faculty from U of L and UK on the project.

Under federal contract requirements, Kentucky was responsible for organizing a large group of Kentucky stakeholders to participate in a number of work groups and committees with specific responsibilities for portions of the project:

- a *steering committee* to oversee the project and develop a plan for implementing recommendations for Kentucky;
- a *Variations Work Group* to assemble organizational-level business practices related to the confidential and secure exchange of health information;
- a *Legal Work Group* to analyze barriers to information exchange and map those barriers back to applicable law and regulation; and

- a *Solutions Work Group* to develop an inventory of possible approaches to dealing with any barriers or other challenges identified.

Kentucky's e-Health Privacy and Security Collaboration Stakeholder Community consisted of more than 60 volunteers and staff from a wide variety of stakeholder organizations and backgrounds. The Kentucky report is a result of this nearly year-long collaborative project. The goal of the project is to assess at the state and local levels how privacy and security practices and policies affect health information exchange (HIE). The main objective of this report is to outline the findings from the assessment of variations in business policy and practice and to provide an overview of various solutions and functional steps possible to address the privacy and security issues that may affect and impede HIE in Kentucky.

Findings and Recommendations

For technology to improve the efficiency and quality of health services to the greatest degree possible, HIE must be largely instantaneous and automatic. This ability is facilitated largely by the use of a set of recognized rules, or standards, among organizations, including standards for protecting the privacy and security of the information. This project identified the following important findings and recommendations regarding the challenges related to various HIE situations.

Widespread Misunderstanding and Confusion Concerning State and Federal Laws on Privacy and Security of Health Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided baseline protections for health information across the United States, but other state and federal laws also contain provisions regarding the privacy and security of protected health information (PHI). Project participants expressed great concern regarding the large number of differing standards and interpretations between state and federal laws protecting health information. Multiple state or federal laws and regulations that deviate significantly from the baseline privacy and security protections that HIPAA provides can be particularly problematic in an electronic information environment.

Health care providers and practitioners in particular expressed a great deal of uncertainty about when patient data may be released and to whom. Issues arose regarding the release of information to payers for administrative purposes, as well as for organizations to monitor patient management. Release of information for nonmedical purposes, such as to police, parents of adult children, employers, marketers, and government agencies, was also particularly problematic.

Issues Related to Handling of Sensitive PHI

Particularly sensitive areas of protected health information include information related to mental health, substance abuse, HIV/AIDS, sexually transmitted diseases, and some other

communicable diseases. These types of sensitive conditions are afforded special protections because of the stigma and potential negative consequences of inappropriate information disclosure. While agreeing that special protections for sensitive health information are important, project stakeholders also noted the difficulty of ensuring compliance with all the provisions found throughout state and federal law related to sensitive PHI. The differing provisions and standards for appropriate disclosure mean that, when in doubt, health organizations do not share any health information. However, this policy could affect greatly both the continuity of care and the quality of care provided as electronic HIE becomes customary. Some participants urged the development of a more coherent set of standards around sensitive PHI. Such standards could have two positive benefits: (1) ensuring to a greater degree that sensitive PHI is afforded the special protections it deserves and (2) making it easier for health organizations to comply with the law.

Technology Limitations Related to Electronic Information Exchange

The project examined many limitations to currently available health information technology (HIT). Identity management is an issue for any technology application, but it is especially important with health information, where life and death matters are at stake. Determining policies and practices for appropriate access, authentication, authorization, and auditing for information systems is critical to protecting the privacy and security of electronic health information. In addition, interoperability is a critical issue to HIE because health information systems currently cannot easily communicate with one another. The lack of a standard way to match patient records across health organizations is another technology challenge. Finally, there are associated problems with the various types of data transfer and with ensuring secure transmission.

Relative Silence in Law on HIE

Much of Kentucky law and regulation governing health care and public health assumes and reinforces a paper-based environment rather than an electronic environment for health information management. Emerging practices such as e-prescribing, HIE, regional health information organizations, and personal health records are so new and dynamic that clear legal parameters simply do not exist yet. Without clear policy guidance, health organizations may be reluctant to move aggressively into the world of e-Health. In some cases, law and regulation may simply be outdated and may not have changed in decades to reflect current practices. The process of updating privacy and security statutes and regulations is difficult because these statutes and regulations are scattered throughout state codes.

Concern Regarding Business Risk and Adverse Legal Action If Information Is Exchanged

The ambiguities between state and federal law, the current limitations to technology, and the newness of e-Health mean that there are inherent risks to early adopters of HIT and

HIE. While many providers, administrators, and practitioners have managed to deal with these challenges, there is an underlying concern that a specific situation may uncover hidden problems and may expose health care entities both to unanticipated risk of their business reputations and to adverse legal action.

A number of solutions were proposed by stakeholders as ways to address the issues and challenges identified through this project. A key means to address the issues and implement proposals will be through the statutorily required Privacy and Security Committee of the e-Health Network Board. This committee will be appointed by the e-Health board in April 2007 and will be charged with addressing the issues identified by the state report, and with implementing recommendations from a state implementation plan (forthcoming). Several categories of action defined in the report are as follows:

- *statutory solutions* requiring the review, revision, or amendment of state or federal laws that are inconsistent with related provisions in state or federal law threaten the feasibility of HIE, or are subject to widespread uncertainty and misinterpretation;

- *regulatory solutions* in areas where regulations may be modified or clarified to facilitate HIE, including confusion or conflict between state and federal regulation and ambiguities that lead to fear of violating a regulation, with associated sanctions or litigation;

- *administrative or organizational solutions* to amend, create, and standardize those health care providers' administrative actions, business policies, and practices that arise because of organizational custom and variation in organizational policies and practices;

- *technological solutions* to improve the secure transmission of health information, improve professional competence regarding the nature and use of digital or electronic communication, and increase the adoption of HIT; and

- *public awareness and education solutions* that promote training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations regarding enhanced quality of care (these solutions address the low level of education about HIE and privacy and security laws, as well as provider concern about business reputation and public relations issues).

LOUISIANA—SUMMARY

Purpose of This Report

In the summer of 2006, the Louisiana Department of Health and Hospitals was awarded a contract by RTI International to participate in the Health Information Security and Privacy Collaboration (HISPC) funded by the US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC); the Agency for Healthcare Research and Quality (AHRQ), and the National Governors Association.

Louisiana is one of 34 states or territories leading local efforts to collect information on business practices surrounding health information exchange (HIE) security and privacy. Collected from a wide variety of stakeholders, the objectives of the project are to

1. identify common barriers to HIE,
2. propose solutions to reduce and eliminate these barriers, and
3. assemble implementation plans to extend the impact of this work beyond the current project.

The final Assessment of Variations and Solutions report provides a summary of the work completed on Objectives 1 and 2 by the Louisiana HISPC state project team and more than 200 stakeholders from throughout Louisiana.

Background on HIT Development in Louisiana

The massive shift of population and loss of medical information after Hurricanes Katrina and Rita made clear the need for interoperable electronic health information in Louisiana. At least 14 major efforts are currently under way in the state, such as the ONC-funded Louisiana Health Information Exchange, the AHRQ-funded Bayou Teche Community Health Net, and the Centers for Medicare & Medicaid Services Doctor's Office Quality IT Project. In addition, several large private multisite systems in Louisiana connect thousands of health providers electronically through proprietary networks. Despite this activity, most providers—especially those in rural areas or in solo practice—do not have access to electronic health information, and most Louisiana consumers do not yet fully benefit from health information technology (HIT) and HIE.

Common to all public and private HIT/HIE efforts in Louisiana are institutional, professional, and consumer concerns with the security and privacy of medical information that will be exchanged electronically at an increasingly rapid rate in ever increasing volumes. While most current public and private HIT/HIE efforts statewide address security and privacy independently of each other, the very nature of interoperability demands that interested stakeholders statewide collaborate on these issues.

Methodology

More than 200 stakeholders from throughout Louisiana participated in the Louisiana HISPC project. Over the course of 8 months, these stakeholders met on a regular basis in order to outline their current health information security and privacy practices, as well as identify barriers to HIE as related to security and privacy practices and their root causes. Stakeholders brainstormed and prioritized solutions to these barriers, using a rigorous process to assess their feasibility and potential impact. Finally, the stakeholders worked to develop work plans to actually put these solutions into practice.

Summary of Top Barriers to HIE

Overall, stakeholders identified and prioritized 38 barriers to HIE. The work groups prioritized these barriers, and the top 11 are as follows:

1. verification of identify, authorization, access control, and auditing
2. variations in standard HIPAA procedures between organizations
3. handling of sensitive protected health information (PHI): conflicting state laws, policies, technical limits
4. unclear distribution of legal liability between entities exchanging PHI
5. Louisiana law as lacking provisions specifically providing an exception for continuity of care
6. handling of patient opt-out: policies, procedures, and technical limits
7. public perception and unawareness of security and privacy rights and obligations
8. authorization for release of PHI for deceased individuals
9. lack of clarity by the courts regarding standards and obligations
10. unclear definition of the *minimum necessary* amount of PHI
11. lack of consensus on who owns PHI

Major Themes

Several major themes were identified during the barrier identification, prioritization, and root-cause analysis process:

1. Large resource and capability gaps exist between payers, hospitals, and smaller providers. While the Health Insurance Portability and Accountability Act (HIPAA) provides for "scalability" to allow for flexibility between different organizations with different missions and means, there is general consensus that outcomes do suffer in smaller organizations where there is not sufficient human capital to implement privacy and security procedures compliant with HIPAA and state law.

2. The type, size, volume, regularity, and clinical importance of information exchanges vary by stakeholder type. This issue has implications for how Louisiana prioritizes the elements in its HIE development process, and a cost-benefit/risk assessment is in order.

3. Differences in identity verification, authorization, access control, and auditing processes may produce security and privacy gaps. Since the chain is only as strong as its weakest link, it was understood that once information leaves the sending organization it is subject to the possibly weaker security and privacy practices of the receiving organization. As HIE efforts expand beyond the 4 walls of large providers into small doctor's offices and other ancillary organizations (or into patients' homes), the number of potential points of vulnerability will increase exponentially.

4. Lack of regulatory guidance and case law results in widely different interpretations of simple HIPAA-driven procedures. In certain cases, the exchange of information between infrequent exchange partners may lead to barriers to the exchange of information. It is likely that variation in interpretation leads to unnecessary costs of implementation and to vulnerability to breaches of confidentiality.

5. Consumers are largely unaware of the issues surrounding health information privacy and security, including their rights and obligations; and providers, government, and other health care entities have little understanding of consumer security and privacy expectations.

6. "Sensitive" PHI is hard to define, and it is procedurally and sometimes technically difficult to carve out. The largest variations between organizations and states may exist here, as well as in the roles and minimum data sets defined by each. Differences in laws and regulations between states may be especially burdensome at border cities.

Summary of Solutions

Once the identification of business practices and barriers to HIE was completed, a second set of stakeholders was asked to convene to develop solutions to these barriers. While 16 detailed solutions are presented in the state report, they may be categorized under one of 4 major solutions:

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

2. Immediately convene current Louisianan HIE/HIT projects to adopt a common security and privacy framework.

3. Promote the adoption of electronic medical records and best-in-class privacy and security practices in small and rural providers.

4. Establish a Health Information Committee under the Louisiana State Law Institute.

Conclusions and Next Steps

The information in this report can only summarize the countless hours of time and effort in and out of formal work group meetings, hours and efforts which were provided by hundreds of stakeholders throughout Louisiana, and it inadequately reflects the strength of the new working relationships and understanding of Louisiana's current HIT/HIE infrastructure and capacity.

Louisiana is further ahead in its HIT/HIE capability and planning than most stakeholders might have believed prior to this project. As a result of Hurricanes Katrina and Rita, Louisiana faces an unprecedented opportunity and challenge to rebuild much of its statewide health system from the ground up. It is expected that the solutions and work plans developed from this effort will be important contributions to this effort, and the hope is that the collaborative effort over the past 8 months will continue to serve Louisiana beyond the life of this project.

At the time of this report, implementation planning is moving forward in conjunction with work resulting from the Region I Health Care Redesign Collaborative and the 2007 Louisiana legislative session. Final work plans will be delivered in the final Implementation Plan report due mid-April 2007.

MAINE—SUMMARY

Background, Purpose, and Scope of Report

The Maine report was designed to provide a synopsis of the solutions proposed by the State of Maine to the business practices identified as barriers to health information exchange (HIE). This report also described solutions for practices that were identified as part of the variations process and that do not necessarily inhibit HIE but do have a privacy and security component to them, specifically in regard to practices surrounding privacy, security, and confidentiality of protected health information.

The Maine state project team also included a description of the extensive dialogue that has occurred over the statewide initiative to integrate clinical information (HealthInfoNet). During the variations identification and compilation process, there were many questions about HealthInfoNet and how it would be governed. The business practices that would relate to this nascent entity were understandably sparse. The Solutions Work Group presented many proposals on how to carry out HIE between stakeholders and a statewide regional health information organization.

Level of Health Information Technology Development in Maine

Maine has been working for the last 2 years on implementing the capacity to facilitate timely exchange of patient clinical information. A 2004 joint publicly and privately funded feasibility study showed strong stakeholder support and diverse community buy-in for integrated electronic health information systems. Following these beginning efforts, Maine's statewide HIE project has continued to plan and develop processes for system governance, technical system requirements, and consumer engagement, while stressing stakeholder involvement and financial support.

Maine's HealthInfoNet project is dedicated to the creation of an integrated statewide clinical-information-sharing infrastructure as a means to improve the quality of health care, enhance patient safety, moderate the growth of costs, and make health care information available to consumers. HealthInfoNet's mission statement calls for an interconnected, secure data-sharing network of health care providers, public health professionals, consumers, payers, and affiliated services, permitting rapid access to patient-specific health care data at the point of care and across networks, hospital systems, and state lines.

Realizing that privacy and security represent core technical components and key concerns that need to be addressed by integrated clinical information networks, the Governor's Office designated HealthInfoNet to respond to the Health Information Security and Privacy Collaboration request for proposal (from RTI International). As one of the state teams awarded this contract, HealthInfoNet has been working throughout Maine in close

collaboration with stakeholders likely to be interested in or affected by an integrated statewide clinical-information-sharing infrastructure.

The goal of the contract is to develop an understanding of business practices in the health care arena throughout the nation, as those practices relate to privacy and security associated with clinical information exchange. RTI shares HealthInfoNet's belief that health care is at its core community based, that its delivery is people-centered, and that practices involving privacy and security of patient information and solutions to these issues will be handled in communities. RTI has provided a common tool set, a structured framework, and a responsive contract liaison to aid in identifying barriers to information interchange and, as the project moves forward, in proposing and implementing solutions to these identified barriers.

HealthInfoNet has assessed variation in information exchange practices for Maine by bringing together key members of the health care delivery community in the state, including providers, payers, state government, public health, emergency medical services, health care legal counsel, laboratories, pharmacies, consumer advocacy groups, and others. It has used this active group of health care experts to propose ways to best resolve practices that are barriers to HIE.

Report Limitations

The state report is inherently limited. Despite many attempts at statewide inclusion, some voices may not have been heard. The state project team remains concerned about the absence of the Veterans Administration (VA) as a voice in this project and has continually reached out to representatives from the VA for direct dialogue. Care providers serving regions of the state with statistically significant Native American populations did provide input on unique issues that interactions with these independent nations may present.

Time, funds, and personnel commitment also remain limiting factors. In spite of these limitations, the state team has found that its regional dialogue about this project with fellow grantees New Hampshire and Vermont, as well as ongoing discussions through conference calls and webb interaction with all the contract grantees, continues to identify recurring and common themes in most areas of statewide HIE.

MASSACHUSETTS—SUMMARY

Several Massachusetts organizations are currently conducting electronic health information exchange (HIE) in the commonwealth. Private-sector organizations have invested significant time and resources in HIE projects that move interoperability forward through both pilot initiatives and production systems.

In the public sector, the Commonwealth of Massachusetts Executive Offices of Health and Human Services (EOHHS) created a webb portal for health and human services programs, known as the *Virtual Gateway.* The Virtual Gateway is intended to provide a single access point to all EOHHS initiatives for consumers, providers, legislators, and researchers.

In accordance with stakeholder input and project team analysis, the Massachusetts Health Information Security and Privacy Collaboration (MA-HISPC) identified 4 issues as key barriers, sources of variations in business practices, or key public policy concerns: (1) patient consent to the use of HIE networks, (2) use and disclosure of sensitive medical information, (3) implementation of access controls, and (4) application of community standards.

In accordance with the state team's analysis of these 4 key issues, the team identified 4 categories of solutions that, when applied to each type of barrier, will markedly advance HIE in the commonwealth: legal, technical, policy, and education. It has identified in each category solutions that will apply to each of these barriers. Additionally, MA-HISPC consistently found that stakeholders manage health information with markedly differing interpretations of the Health Insurance Portability and Accountability Act, other federal laws, and state laws. Thus, a set of solutions around policy development that will support operations and education for the consistent implementation of these laws is in order. Finally, the development and implementation of a comprehensive communication strategy was identified as a critical component of all future work.

After further consideration of these 4 barriers, MA-HISPC has now focused its implementation planning on two priority areas: (1) patient consent for the use of HIE networks and (2) use and disclosure of sensitive health information. MA-HISPC feels that each area must be addressed through legal, technical, policy, and educational solutions. At each stage of the work and discussions—Variations Work Group, Legal Work Group, Solutions Work Group, and now Implementation Plan Work Group—the MA-HISPC project determined that these two areas need to be addressed before true interoperable electronic HIE is possible in Massachusetts. The recommended solutions and implementation plan include the following elements.

For the area of patient consent,

- develop a common understanding of state laws and regulations as related to patient consent and as applied to information networks and HIE;
- ensure that future HIE systems will be able to capture and share patient opt-in and other preferences, capture patient consent at one point in the system and flow this information to all clinicians and clinical points of care, and record and implement changes in consent with changes in patient's medical and clinical conditions;
- establish industry consensus policies and procedures addressing patient consent and sharing of patient consent, to be implemented with a flexible framework across the HIE enterprise, including policies to enable consent at one point of care to appropriately flow to all clinicians and clinical points of care; and
- address current and continuing education needs regarding state and federal laws and regulations.

For the area of sensitive health information,

- develop common understanding of state and federal laws and regulations related to sensitive health information;
- develop and disseminate uniform definitions of sensitive health information, definitions based on state and federal laws;
- identify the technical needs for sensitive information management within an electronic health record (EHR) and regional health information organization (RHIO), along with baseline business and technical policies that must be in place for sensitive information management.
- ensure that future electronic HIE systems will be implemented with a flexible framework to enable identification and classification of sensitive information within databases, creation of sensitivity flags for use in the EHRs and RHIOs, and the use (when applicable) of data-filtering technologies to filter sensitive information on the basis of state laws and regulations;
- ensure that future HIE systems will be able to flag sensitive data (in general and in a specific patient's electronic records) and block external access to internally flagged sensitive data actions, capabilities which should be coupled with effective communication to system users that some kinds of information may be blocked (so that clinicians can use the system appropriately with patients); and
- address current and continuing education needs regarding state and federal laws and regulation.

The MA-HISPC has developed a preliminary implementation plan that includes use-case scenarios and work groups to develop clinical, policy, legal, and technology work product. The plan will be shared with communications and education task forces to inform their processes. This work will enable implementation of solutions while Massachusetts coordinates its work with other states and with national initiatives.

MICHIGAN—SUMMARY

The purpose of this summary is to document the Michigan Health Insurance Security and Privacy Collaboration (HISPC) team's assessment of variations and solutions regarding privacy and security barriers in the electronic exchange of health data. By discussing the scenarios provided by RTI with a comprehensive group of stakeholders from all regions in the state, the Michigan HISPC state project team was able to identify, categorize, and summarize a list of 10 major barriers for discussion by the Solutions Work Group.

The Solutions Work Group consisted of a broad spectrum of health care–related stakeholders and volunteers from the variations participants. In addition, extensive research into consumer reaction was included in Michigan's final report.

One of the team's biggest challenges was managing the size and complexity of Michigan. Michigan has a diverse population, which represents more then 80 different nationalities, cultures, and ethnicities, including a wide array of socioeconomic groups and every major form of health care delivery. Fifty-seven of Michigan's 85 counties are rural, where some of our most advanced work is being developed in health information exchange (HIE). Michigan's urban center, Detroit, leads the list of underserved populations, while our suburban centers provide cutting-edge delivery just a few miles away.

Additionally, this project helped foster interest in the governor's commitment to improving Michigan's quality of care and patient safety by utilizing HIE. In the original proposal, Michigan states that "the State of Michigan is pleased to be included in the work of this project as it aligns with the goals and mission as set forth by Governor Granholm to advance health care into the 21st century using technology to effectively, efficiently and privately share critical health information in Michigan." The absolute truth of this statement grew to almost monumental proportions during the course of this engagement. The Michigan HISPC project helped foster, or at least provided support to, the following related projects.

The Michigan Health Information Network Conduit to Care

In April 2006, the Michigan Department of Community Health (MDCH) and the Michigan Department of Information Technology (MDIT) brought together Michigan stakeholders to develop a vision and plan for the future of health information technology and exchange in Michigan, a report called the Michigan Health Information Network (MiHIN) Conduit to Care.

The report is a roadmap for engaging all regions of the state in HIE that will allow for the efficient, secure, and electronic transfer of health information between disparate entities involved in a patient's care. With the patient's consent, pertinent health information can be

available to physicians at the point of care. The overall goal for the MiHIN initiative is to improve the overall quality of health care and increase patient safety.

MDCH and MDIT are currently working with the MiHIN participants to prioritize recommendations and develop strategies for moving forward.

Health Information Technology Commission

In May 2006 the Michigan Health Information Technology Commission was created by Public Act 137-06 as an advisory commission within the MDCH. The mission of the commission is "to facilitate and promote the design, implementation, operation, and maintenance of an interoperable health care information infrastructure in Michigan." The health information technology (HIT) commission was appointed by the governor in August 2006 and met for the first time in October 2006. Each commissioner represents a class of stakeholders, including consumers, providers, payers, employers, and hospitals, among others. The HIT commission plans to work with communities and stakeholders to reduce barriers and challenges to HIE and promote the growth of HIE across the state.

All HIT commission meetings are open to the public; the commission therefore has been able to encourage stakeholder feedback at each of its meetings. Also, the commission has invited and plans to continually invite regional HIEs to present information to the commission about their initiatives and the challenges and successes they have experienced.

Michigan HIE Resource Center

The Michigan HIE Resource Center will be focused on assisting the regional HIE efforts across the state by providing assistance and knowledge in order to increase the adoption rate and successful implementation of regional HIEs across Michigan.

Using a portion of the $5 million available in the fiscal year 2007 MDCH budget, MDCH issued a request for proposals in December 2006 to implement the Michigan HIE Resource Center. Proposals were due at the end of January 2007 and awarded in March 2007.

The HIE Resource Center will play a major role in supporting regional information exchange, a critical component of health care efficiency, by offering guidance to align with national standards, resolving any conflicts between regional HIEs, and facilitating equitable and appropriate data sharing for the benefit of patients.

The HIE Resource Center will support the State of Michigan's role as convener and collaborator for Michigan HIE. This centralized body will have the ability to bring different regional exchange initiatives together by providing parameters, guidelines, and support, bridging gaps between regional efforts that are in various stages of development. The Resource Center will promote sustained efforts to (1) build governance structures; (2) coordinate national, state, and local efforts; (3) promote education; (4) foster collaboration

among stakeholders; (5) raise consumer awareness; and (6) develop financial and human resources. It will engage a variety of people, including full- and part-time staff, work group volunteers, student interns, subject matter experts, faculty, and consultants to keep abreast of national trends and local issues. Participants from previous and ongoing efforts, including MiHIN work groups, State of Michigan departments, local regional health information organizations, and participants in the HISPC project, will be drawn upon to move the process forward.

Regional HIEs Implementation and Planning Grants

Michigan's fiscal year 2007 MDCH budget contains $5 million to support regional HIE initiatives. In December 2006, MDCH released a request for proposals to provide planning or implementation grants to support Michigan regions in the HIE endeavor. The grants are due to be awarded in April 2007.

MINNESOTA—SUMMARY

In 2005 the governor and the Minnesota legislature made e-Health a state priority by establishing the Health Information Technology and Infrastructure Advisory Committee (Minnesota e-Health Advisory Committee)[5] in Minn. Stat. § 62J.495. The Minnesota e-Health Advisory Committee is charged with advising the commissioner of health on health information technology issues and goals. One of the committee's responsibilities is to address critical issues related to the security and confidentiality of health information and patient privacy requirements in this new era of electronic health information exchange. The Minnesota Privacy and Security Project (MPSP) is a first step in fulfilling this responsibility.

Health industry stakeholder and consumer involvement in the MPSP has been critical to ensuring that project results are broadly acceptable and applicable to the community. The MPSP was structured to provide all interested individuals the ability to participate directly and follow the project activities through its website at http://www.health.state.mn.us/ehealth/mpsp/index.html.

The MPSP was launched with Minnesota's award of a Health Information Security and Privacy Collaboration (HISPC) contract to examine privacy and security issues related to health information exchanges. The HISPC contract is part of a US Department of Health and Human Services project titled, Privacy and Security Solutions for Interoperable Health Information Exchange.[6] The Minnesota e-Health Advisory Committee serves as the steering committee for the activities of the HISPC contract.

Under the Minnesota e-Health Advisory Committee's direction, the MPSP conducted a systematic and comprehensive review of current laws and practices to identify the most significant privacy and security barriers facing organizations in the implementation of electronic exchange of health information.

The state's final report was an integration of the MPSP's first two reports titled, Privacy and Security Barriers to the Electronic Exchange of Health Information, and the Interim Report on Solutions to Barriers to the Electronic Exchange of Health Information.

At the end of the project's first phase in October 2006, the MPSP issued a report titled, Privacy and Security Barriers to the Electronic Exchange of Health Information. This report identified the two most significant privacy and security issues that must be solved to advance the appropriate electronic exchange of health information:

[5]More information on the Minnesota e-Health Advisory Committee's activities can be found at http://health.state.mn.us/e-health.
[6]Contract #290-05-0015 from the Agency for Healthcare Research and Quality.

1. The implementation of Minnesota's patient consent requirements within a health information exchange is an issue:

   – First, there are significant and irreconcilable differences in organizations' interpretations of Minnesota's patient consent requirements. These differences make it impossible for health care providers to agree on "when" and "how" patient consent is required.

   – Second, the patient consent requirements were designed for paper-based exchanges of information and early electronic data base systems that are not conducive to a real-time, automated electronic exchange of information.

2. Operational difficulties in first providing and then limiting and monitoring external organizations' electronic access to patient data is an issue. This issue is identified as one general issue, because it is a set of interconnected security problems that must be addressed concurrently to successfully implement a health information exchange. To give external health care providers appropriate access to electronic health records and patient data, organizations need to address 4 security topics, for which there are no fully adequate solutions:

   – mechanisms to establish and maintain a list of individuals authorized to access patient data;

   – methods to authenticate authorized individuals who access patient data;

   – information access controls—within information systems and through coordinated organizational policies—to limit authorized individuals' access to the patient data that is appropriate for the individual's functions and needs; and

   – mechanisms for coordinated auditing across organizations to identify authorized individuals who inappropriately access health information.

During the second phase of the project, the MPSP convened a Solutions and Implementation Plans Work Group to develop solutions that eliminate or reduce these two privacy and security barriers while preserving and strengthening patient privacy protections. The Solutions and Implementation Plans Work Group formed two subgroups to address each of the barriers individually.

The Patient Consent Subgroup

The Patient Consent Subgroup examined differences between health care providers' interpretations of requirements for patient consent to exchange patients' health information. This subgroup proposed a number of modifications to Minn. Stat. § 144.335 to resolve differences between health care providers regarding "when" and "how" patient consent is required in order to exchange patients' health information. The potential solutions address 9 specific patient consent issues by

- defining undefined terms and ambiguous concepts in Minnesota's patient consent requirements;

- adding language to clarify the application of Minnesota's patient consent requirements to new concepts in the electronic exchange of health information; and

- updating Minnesota'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.

The Authorization, Authentication, Access Control and Auditing Subgroup

The Authorization, Authentication, Access control and Auditing Subgroup developed a set of 19 principles for authorizing and authenticating individuals, setting access controls, and auditing in a health information exchange. These principles provide Minnesota health care organizations a foundation and framework for the continued development of health information exchanges and can guide organizations' decision making in forming and implementing health information exchanges. The general principles form a "conceptual solution" that was developed to be

- independent of a particular health information exchange architecture;
- flexible enough to adapt to changes in information technology;
- consistent with national standards currently under development; and
- capable of being refined and more finely detailed as health care organizations gain experience in implementing the electronic exchange of health information.

The efforts of these two subgroups will help to eliminate or reduce the two most significant privacy and security barriers to the electronic exchange of health information in Minnesota. In April 2007 the MPSP will issue a final implementation plans report that identifies and describes mechanisms and plans for implementing the solutions outlined in this earlier work.

MISSISSIPPI—SUMMARY

As the use of health care technology expands in complexity and in provider dependence on technology for care, the creation of an interoperable information network for the secure exchange of patient information becomes increasingly important. The creation of a centralized, secure, interoperable information network utilizing fully functional EHRs has the potential to improve the efficiency and efficacy of health care delivery by improving health outcomes and decreasing costs. As noted by David Brailer, the former National Health Information Technology coordinator, the United States is in the process of creating a "point of care" information network by which practitioners and clinicians will have real-time access to critical health care data to improve patient care and safety. Standards regarding the way information is transferred, the type of information to be transferred, and privacy and security issues surrounding this information must be addressed in an inclusive manner.

In February 2006, RTI International released a request for proposal entitled, Health Information Security and Privacy Collaboration (HISPC). This project is part of a national collaborative involving the National Governors Association; the US Department of Health and Human Services, Office of the National Coordinator for Health Information Technology; and the Agency for Healthcare Research and Quality. The Office of the Governor for the State of Mississippi designated Information & Quality Healthcare (IQH) as the entity to apply for the subcontract with RTI. IQH, together with 33 states and a single territory, was notified in May 2006 that its proposal to represent Mississippi on the HISPC initiative had been accepted.

The Foundation for eHealth Initiative conducted a preliminary assessment in 2006 of health information exchange in Mississippi. This preliminary assessment found that information technology (IT) integration in rural Mississippi reflects IT integration in rural America in general. The transfer of personal health information is limited to fax or e-mail. Few rural health care providers have a fully integrated EHR. Consequently, the secure and timely electronic transfer of protected health information (PHI) is limited by the lack of connectivity, lack of health information technology (HIT) integration, lack of trained IT personnel, and lack of funding.

The eHealth Initiative, the Southern Governors' Association Gulf Coast HIT Task Force, and the HISPC Interim Assessment of Variations report show that there are varying degrees of regional or community-specific health information exchange (HIE) activities in the state (24 HIT/HIE activities are currently under way in Mississippi, and several of these were initiated in the aftermath of Hurricane Katrina); there are silos of HIE activity with possibly some crossover; and there is no coordinated statewide HIE activity. No centralized entity currently

exists in Mississippi to oversee the implementation of a secure, integrated, interoperable health information network and infrastructure.

The HISPC initiative requires 4 broad tasks for IQH to undertake: Task 1—Assess variation in organizational-level business policies and state laws regarding the transmission of health information, and identify barriers, business practices, or policies which impede health information exchange; Task 2—Formulate interim solutions and implementation plans to overcome the barriers; Task 3—Formulate final solutions and implementation plans; Task 4—Manage the project. To accomplish the tasks in the initiative, 4 work groups have been established: Variations Work Group in assessment of business practices; Legal Work Group; Solutions Work Group; and Implementation Planning Work Group.

Mississippi recommendations fall within 4 major categories: (1) solutions affecting variations in business practices and policies; (2) solutions affecting state laws or regulations; (3) solutions affecting federal laws or regulations; and (4) solutions affecting interstate HIE. Recommended solutions include the following:

- Create a centralized authority to oversee statewide HIE and HIT development and adoption, and to oversee the development of standardized policies, procedures, and contract terms for business associate agreements.

- Develop a centralized authority that will establish a health information infrastructure work group. The work group will assist health care organizations in adopting standard terminology, data forms, and exchange protocols. In addition, the work group will assist health care organizations in the implementation of national standards and guidelines for HIE.

- Develop a centralized authority that will have responsibility to support education for providers, insurers, consumers, and other involved parties regarding the legal interpretation of state and federal laws and regulations governing the exchange of private and secure health information; provide a hotline for call-in questions; provide a website; and work with trade associations to provide continuing education.

- Develop a centralized authority that will be responsible for identifying state law changes necessary to facilitate HIE in Mississippi, including presentation of proposed statutory changes to the legislature annually. This centralized authority would establish a legal work group to represent all stakeholders in developing proposed language for legislation to address appropriate laws.

- Use national guidelines to establish statewide standards. These standards would provide a framework for intrastate and interstate transmission of PHI.

NEW HAMPSHIRE—SUMMARY

The New Hampshire state project team did not include an executive summary.

NEW JERSEY—SUMMARY

The New Jersey final Assessment of Variation and Analysis of Solutions report was submitted by the state project team to RTI International, pursuant to Health Care Research and Quality Contract 290-05-0015.

The objective of this contract is to assess how privacy and security laws and business practices affect the exchange of interoperable health information; to examine how privacy and security policies and business practices regarding electronic health information impact the exchange of said information; to convene and work closely with a wide range of stakeholders in New Jersey; and to develop an implementation plan to address organizational-level business practices and state laws that affect the private and secure interoperable exchange of protected health information (PHI). In New Jersey, the PHI concept is also linked to the New Jersey Information Practices Act, and the scope of information subject to privacy and security protections by certain industry parties may actually be broader than the Health Insurance Portability and Accountability Act (HIPAA) federal use of the term *PHI.*

Furthermore, all aspects of HIPAA's Administrative Simplification requirements and procedures are part of New Jersey's prompt payment and clean claim laws, which apply to the payment of medical claims. The New Jersey Department of Banking and Insurance is the regulatory authority over these issues. What has emerged in New Jersey is a unitary business model in which questions of privacy, security, the implementation of the transaction and code sets, claims payment practices, coordination of benefits, and many other issues have an impact on the timely payment of clean claims. Hence, all parties—providers, payers, institutions, clearinghouses, third-party billers, third-party administrators, pharmacy benefit managers, and many others—must work together from the inception of the medical encounter to create practices and procedures that work efficiently and do not interfere in the timely payment of clean claims.

The state's final report refines and expands on two interim reports submitted earlier in the project, namely, the Interim Assessment of Variations report and the Interim Assessment of Solutions report. This report presents final project conclusions on the business practices and policies affecting secure exchange of PHI in the state, barriers to such exchange, and proposed solutions developed by the various project work groups.

During the course of the project, the state project team identified and consulted with many different stakeholders representing a variety of providers, payers, government agencies, and consumer groups. For the assessment of both the variations in business practices and the development of solutions to secure health information exchange (HIE), appropriate stakeholders were asked to review and respond to HIE scenarios and domains provided by

RTI. In order to solicit responses, individual interviews, group meetings, and conference calls were conducted, each of which was documented and reported by the state project team.

Most of our original conclusions contained in the Interim Variations and Solutions report have remained the same. However, some new health information technology activities have been launched in New Jersey, including the development of a business plan for a regional health information organization (RHIO) and other such efforts. The state's report includes information about these activities. The New Jersey Department of Banking and Insurance and the state project team see this surge in forward momentum as a direct result of the work undertaken in this initiative.

The final findings on variations in privacy and security practices and findings on solutions to identified barriers to secure HIE are as follows:

- In some instances some identified processes and procedures are deemed to be "appropriate controls" on the dissemination and exchange of PHI, even though they create a barrier to the rapid exchange of medical information.
- In multistate situations, discussions with a number of stakeholders disclosed uncertainty and confusion regarding the application of the appropriate state's law pertaining to the consent requirements for the release of PHI associated with treatment, payment, and health care operations.
- In addition, after meetings with stakeholders, the state team has observed that HIPAA is itself often misunderstood by stakeholders as requiring creation of barriers or time-consuming privacy and security processes when none exists.
- Many stakeholders disclosed difficulty and confusion regarding the application of and compliance with HIPAA's *minimum necessary use* test in real-life circumstances including providers who think it applies to the treatment scenarios.
- Many technical and infrastructure barriers to electronic interoperability were identified.
- Many providers expressed a high level of comfort with and acceptance of the existing business practices pertaining to PHI data exchange, such as telephone consultation, faxed documents, and paper records. They do not yet fully recognize the efficiencies, benefits, and quality-of-care improvements that will flow from interoperability of electronic health records.
- Some providers expressed a lack of certainty that more automated electronic processes would present substantial savings in the delivery of medical care in relation to the cost of implementation. These providers have advised the New Jersey project manager that they recognize the potential savings for payers, but they are skeptical about the return on investment for providers.
- Financial resources and staffing limitations available to providers are frequently cited as an impediment to interoperability.

- Stakeholders identified specific categories of highly personal and "sensitive" PHI, such as sexually transmitted diseases, AIDS/HIV, mental and emotional health (including psychotherapy notes), substance abuse, and genetic testing data, which create special challenges for state and federal law and practice and may require special situational rules for access, inclusion, and interoperable exchange of this kind of PHI.

Section 6.0 of the state report presents and analyzes the state project team's identified solutions. These solutions are presented in 5 categories:

- interoperability,
- work flow,
- federal and state law,
- HIPAA security and privacy, and
- education.

The *interoperability* solution category includes the technology imperatives and the standards support required for smooth sharing of medical and administrative information. The stakeholders understand that technology may not yet permit enterprise-wide solutions and that not all standards necessary for interoperability are yet in place. Despite these restrictions, the stakeholders have identified the technical functionality necessary for interoperability and necessary to implement electronic systems in the near future, including

- encryption and authentication standards,
- statewide uniform security protocols,
- standardized secure webb portal solution,
- stratification of information access, and
- strong auditing measures.

New Jersey does not yet have a functional regional health information organization, but there are a number of state and private networks and projects working on sharing medical and administrative data electronically, which are expected to provide a basis for devising statewide solutions.

The New Jersey *work-flow* solution category highlights a number of changes and adjustments possible in an office work flow during the provision of medical services, changes that will permit smoother interoperability and more complete record keeping.

The New Jersey state team anticipates developing a number of community-based standards and best practices. These will be developed though community forums. Community forums may be held with consumers and stakeholders to discuss work flow and collect information.

From these forums a typical work flow will be developed, and a set of consensus best practices and standards may be developed. Unusual work flows will also be outlined for statewide use. The team is hoping that additional funding will be provided by the federal authorities in the form of follow-on Health Information Security and Privacy Collaboration (HISPC) contracts to facilitate these implementation plans.

The New Jersey health care stakeholders need continuing education and update training to understand the *federal and state laws and regulations* that impact health care within the state. Currently, there is a great deal of confusion, misunderstanding, lack of knowledge, and breadth of interpretation of the health care laws and regulations in New Jersey.

Federal and state law management will consist of several prongs, as follows:

- There should be statewide understanding and interpretation of federal and state health care laws and regulations, and the ability to access these federal and state health care laws and regulations from a single database when necessary.
- There should be a statewide consensus baseline of the policies and procedures in place for federal and state health care laws and regulations, mandates, and requirements.
- The provider licensing and renewal requirements may need to be amended to include provider education, as well as continuing education, on federal and state health care privacy and security laws and regulations. There should be consensus policies and procedures to dispel myths, address cultural issues, and address the differing perceptions between and among the provider and payer stakeholders—and how they may differ from consumer perceptions.

The *education* solutions are initial and critical foundation blocks to HIE and interoperability in New Jersey. The Solutions Work Group, steering committee, and project management staff agree that an education package should be developed to assist with dispelling cultural and perception barriers. The federal and state HIPAA laws and regulations, as well as policies and procedures developed and approved for New Jersey, should be explained to the consumer and provider stakeholders, as well as to all the other stakeholders, for statewide understanding.

The state team implementation planning process will consider and investigate a number of outreach and communications methods and efforts, including

- face-to-face training;
- community forums;
- town hall forums;
- teleconferences;
- WebEx presentations and conferences;

- newsletters;
- postings of news and alerts to websites and portals;
- brochures;
- mass media; and
- properly trained and supplied state and provider trade association speakers bureaus, which should be available to present wherever needed.

Any education programs and packages will be available for the stakeholder community for use inside their own institutions and facilities.

All documents and outlines developed to support solutions will be accessible and available to the New Jersey health care community for all to review and download.

The New Jersey state team interim implementation plan considers all the items and ideas presented here.

The state team is currently evaluating the feasibility of proposed solutions. It plans extensive discussions with stakeholders regarding feasibility, since not all affected stakeholders in New Jersey have participated in the HISPC project. In addition, many of the proposed solutions will require extensive effort and expense. More education within the state about the potential benefits of HIE will be necessary to develop a consensus among the many interested parties, and pilot approaches will be necessary to test the feasibility of some solutions. While some entities have developed their own electronic health records, using these records as building blocks for a statewide system will require extensive political buy-in.

Because many different departments and agencies are concerned in the delivery of medical care, handling PHI, and related issues, it is important for all New Jersey governmental agencies to actively and continually communicate with each other on all issues that impact health care issues. All websites should be cross-linked and should be monitored for consistency of information and message.

NEW MEXICO—SUMMARY

New Mexico is a primarily rural state with a large geographic area. It has a total population of about 1.8 million; one large metropolitan area, Albuquerque, with approximately 700,000 people; and a number of small cities and towns, most with populations of less than 50,000. The development of the health information exchange (HIE) network has been under way for two and a half years, led by the New Mexico Health Information Collaborative, a community-based initiative funded by the Agency for Healthcare Research and Quality, community partners, and the New Mexico State Legislature. The Master Person Index, record locator services, data engines, and patient referral services have been in pilot test in Taos, New Mexico, since October 2006. The large health systems in Albuquerque are in the process of implementing electronic health record systems, and there are pockets of EHR system adoption in the small cities and towns, but most practices, especially small ones, continue to be paper based.

The Variations Work Group (VWG) included representation from a diverse set of stakeholder groups. These stakeholders identified 165 privacy and security business practices and concluded that 37 of them posed impediments to electronic HIE. The Legal Work Group reviewed the results from the VWG and made 5 key observations:

- Various specific New Mexico statutory provisions have a negative effect on the potential for interoperable HIE.
- There is a lack of certainty as to whether the Health Insurance Portability and Accountability Act (HIPAA) or a specific state law may apply in certain situations.
- Inconsistencies between HIPAA and state law requirements may result in inconsistent approaches.
- The lack of a comprehensive approach under New Mexico state law to the use and disclosure of health information results in numerous fragmented statutory provisions with different requirements.
- The complexity and lack of a comprehensive state law approach leads to potential misinterpretations of the applicable standard.

New Mexico solutions to HIE barriers fall within the following categories:

1. variations in organization business practices and policies (Section 6.1)
2. state laws and regulations (Section 6.2)
3. federal laws and regulations (Section 6.3)
4. interstate HIE (Section 6.4)
5. national-level recommendations (Section 7.0)

Recommended solutions included the following:

- Shared or centralized authentication services should be developed: Explore ways to standardize and possibly centralize authentication services for the HIE network throughout the state.

- Secured messaging is needed: Implement a shared secured messaging platform for HIE networks.

- Standardized HIE contractual agreements are needed: Develop and adopt standardized forms, address liability issues, and establish use agreements with defined rights and responsibilities.

- Updates to state laws and regulations are needed: The State of New Mexico proposes to create new legislation that will protect the privacy of health care information when it is stored or transmitted electronically. If the new privacy legislation modifies certain sections of previous laws, the new legislation will also note these changes.

- Privacy and security education for providers and payers is needed: Provide privacy and security education for health care providers and other health care organizations.

- Privacy and security education for patients and consumers is needed: Although state organizations can disseminate information to patients and consumers regarding their federal and state privacy rights, the federal government must assume leadership to create and distribute a consistent educational message nationwide. This education should also include the benefits of health information technology, such as improved quality of care and patient safety, as well as lower cost.

- Policies, practices, and standards for communication between HIE Networks (including Master Patient Indices) are needed: In order to establish interoperability between local HIEs and the Nationwide Health Information Network (NHIN), national policies, practices, and standards must be developed. National policies and practices will probably have to be prerequisites because they set forth the context within which message format standards and data content standards are created.

- National policies, practices, and standards are needed for authentication and authorization: Provide support for professional and industry associations, as well as for standards development organizations, to develop nationwide policies, practices, and standards for authorization and authentication. These steps are necessary to accelerate the development of regional health information organizations and the NHIN.

- Updates to HIPAA privacy and security regulations are needed: Work with the federal government to extend HIPAA privacy regulations beyond the designated covered entities to address requirements for a privacy framework applicable to state and regional HIE systems.

NEW YORK—SUMMARY

It has been said that the brick and mortar 20th century health care delivery system will be replaced in the 21st Century with a health information and communications technology infrastructure accessible to all patients and providers.[7] Enabled with clinical decision support tools and powered by interoperable technology, this infrastructure offers the opportunity to improve the quality and efficiency of the care delivered while giving consumers better control over their health care experience.

Strong policies that protect the privacy and security of health information are crucial to achieving this transformation. Patients share a great deal of sensitive personal health information with their physicians and caregivers. This information is then shared with insurance companies, pharmacies, researchers, and government for reasons such as treatment, payment, public health, and research. Without adequate privacy protections, individuals take steps to shield themselves from harmful and intrusive uses of their health information, often at significant cost to their health. A consumer-oriented privacy and security framework that ensures that personal health information is used in an appropriate and transparent matter is essential to earning the trust of patients and to the ultimate success of electronic health information exchange (HIE).

Current laws governing HIE and the resulting business practices were developed in the context of a paper world where decisions on what to communicate, how, and to whom are generally made on a one-to-one basis by clinicians. The current laws attempt to serve the patient's privacy interests by restricting what can and cannot be shared and restricting the terms on which sharing takes place. Human judgment and personal relationships play a major role, as clinicians attempt to act as the guardians of their patients' information. However, from the standpoint of the patient's health and wellness, the system falls short. Patients have difficulty accessing their own personal health information and ensuring its availability at the point of care.

Moving from a paper to an electronic health system changes the information-sharing dynamic. An interoperable health information system facilitates a many-to-many relationship, enabling different information technology systems and software applications to exchange data accurately, effectively, and consistently. This change offers new opportunities for patients' access to and control over their health care information, and it facilitates the safety, quality, and efficiency of their care. However, it also demands new approaches for protecting patient privacy and security, including policies addressing the disclosure and use of health care information, and technologies that address patient

[7]Institute of Medicine. To err is human: Building a safer health system [Institute of Medicine website]. November 1, 1999. Available at: http://www.iom.edu/?id=12735. Accessed May 9, 2007.

identification, authentication, record location, identity management, and storage of special classes of information.

The New York state report examines the current laws and business practices related to privacy and security of health information in a paper-based world and begins to explore their implications for the transition to electronic HIE.

NORTH CAROLINA—SUMMARY

Background

In April 2004 President George W. Bush articulated his vision for the future of health care in the United States by an executive order that authorized the secretary of the Department of Health and Human Services, Michael Leavitt, to establish the Office of the National Coordinator for Health Information Technology (ONC), which provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety.

In October 2005 ONC and the Agency for Healthcare Research and Quality awarded the Privacy and Security Solutions for Interoperable Health Information Exchange contract to RTI International. RTI, in collaboration with the National Governors Association Center for Best Practices, formed the Health Information Security and Privacy Collaboration (HISPC) project and invited the states and territories to submit proposals to participate in the project. The HISPC project was designed to examine privacy and security laws and business practices that affect the ability of every state and territory to exchange electronic health information within its borders and with other states.

The North Carolina Healthcare Information and Communications Alliance (NCHICA) submitted a proposal and in April 2006 was awarded the contract to represent North Carolina. Since the project's commencement, teams of health care stakeholders have worked collaboratively through a process of consensus to identify, assess, and develop plans to address variations in organizational-level business policies and state laws that affect privacy and security practices that may pose challenges to health information exchange (HIE).

Purpose

The purposes of the North Carolina HISPC project are to address variations in organizational-level business policies and state laws that affect privacy and security practices which, in turn, may pose challenges to interoperable HIE; to recommend solutions and implementation plans to reduce or eliminate these challenges; and to increase the level of expertise in and compliance with privacy protections within the health care community.

North Carolina HISPC's goals are to

1. identify current health care practices and challenges regarding the release and exchange of health information,

2. develop consensus-based solutions for interoperable electronic HIE that protect the privacy and security of health information, and

3. recommend high-level plans to implement recommended solutions.

The state project team recommends policy, technological, and legal solutions to the barriers or obstacles identified in the Assessment of Variations report. In addition to identifying solutions, the report also documents, for each potential solution, the HIE context, privacy and security domains affected, involved stakeholders, HIE barriers that are addressed, and each solution's current stage of development.

Work Group Composition

The Variations, Legal, Solutions, and Implementation Work Groups comprise attorneys; practice managers; researchers; clinicians; and professionals in public health policy, health information management, and information security who specialize in health information privacy and security and who represent health care stakeholders such as consumers, health plans, professional organizations, health care facilities, laboratories, health care software vendors, and public health agencies.

The Variations Work Group (VWG) conducted individual and group assessments to document the stakeholders' current practices if they were presented with each of the 18 health care scenarios provided by RTI. The VWG was charged with collecting the business practice data and identifying potential barriers to exchanging health information. The VWG was chaired by Jim Murphy from the North Carolina Department of Health and Human Services (NC DHHS), Office of Medicaid Management Information Systems; Mike Voltero, General Counsel to Blue Cross Blue Shield of North Carolina; and Roy H. Wyman, Jr., a partner at the law firm Maupin Taylor Williams Mullen.

The Legal Work Group (LWG) analyzed the business practices provided by the VWG and identified legal sources of the barriers to exchanging health information. The LWG was chaired by Patricia A. Markus, a partner at the law firm Smith Moore, LLP. The LWG was composed of members representing the following stakeholders: Blue Cross Blue Shield of North Carolina, CareSpark, FirstHealth of the Carolinas, LabCorp, Williams Mullen Maupin Taylor, NC DHHS Department of Medical Assistance, North Carolina Hospital Association, NC Medical Society, Pitt County Memorial Hospital, North Carolina Health Information Management Association, Quintiles Transnational, MISYS, North Carolina Office of Information Technology Services, and UNC Hospitals.

The Solutions and Implementation Plan Work Groups (SWG and IPWG) reviewed the data collected from the VWG and developed solutions and implementation plans to reduce or remove the identified barriers. The SWG and IPWG were chaired by Dave Kirby, president of Kirby Information Management Consulting. The SWG and IPWG were composed of members representing the following health care stakeholders: Blue Cross Blue Shield of North

Carolina, Duke University Health System, eHealth Initiative, E-Tech Security Pro, NC DHHS Office of Medicaid Management Information Services, North Carolina Department of Mental Health and Substance Abuse, Novant Health, and Radarfind.

With the exception of the project management office (PMO), all project participants voluntarily contributed their time and expertise to this project.

Methodology

RTI provided the state project team with 18 scenarios to analyze along 9 domains of privacy and security. Each scenario represented a business practice or health care scenario that required the exchange of health information between different entities within North Carolina or between North Carolina and other states. The state project team grouped the 18 scenarios into 4 subgroup work clusters based on the type of stakeholders interviewed, the legal sources for the barriers, the security domains relevant to the scenarios, and the field of expertise of each professional participant.

The scenarios' 4 subgroup work clusters are as follows:

Subgroup 1: Patient Care Scenarios

1. Patient Care A (Emergency Transfer)
2. Patient Care B (Substance Abuse)
3. Patient Care C (Access Security)
4. Patient Care D (HIV and Genetics)

Subgroup 2: Payer Scenarios

5. Payment (Electronic Health Record Access)
9. Pharmacy Benefit A (Mail Order)
10. Pharmacy Benefit B (Claims Savings)

Subgroup 3: Secondary-Use Scenarios

6. Regional Health Information Organization (Data Access)
7. Research (Data Usage)
8. Law Enforcement (Test Results)
11. Operations and Marketing A (Rehab Center)
12. Operations and Marketing B (Birthing PHI)
14. Employment Information (Return to Work)

Subgroup 4: Government Public Health and Safety Scenarios

13. Bioterrorism Event (Anthrax Spread)
15. Public Health A (Active TB Carrier)

16. Public Health B (Newborn Screening)
17. Public Health C (Homeless Shelters)
18. Health Oversight (Legal Compliance)

The PMO developed a facilitator training program to ensure that interviewees were comfortable sharing the policies and practices of their organization during the assessment interviews. The training program elements included confidentiality reassurance, guidance to maintain objectivity, suggestions for how to focus discussions on the presented scenarios and work session questions, and suggestions for recapping information for the recorders. Each VWG session was facilitated and recorded by one or more of the project chairpersons, the project manager, and the project coordinator.

In preparation for the assessment sessions, the chairpersons formulated 7 questions to focus on the "who, what, how, and why" of the organization's business practices regarding the sharing of information that correlated to the assessment-tool fields. The questions each interviewee was asked are as follows:

1. What is your stakeholder type?
2. What is your current business practice if presented with this type of scenario?
3. Why is that your current business practice?
4. Does this business practice aid the exchange of health information with other entities?
5. Does this business practice present a barrier to exchanging health information?
6. Is this barrier appropriate to safeguard the information?
    a. Why is it appropriate?
    b. If not, could you recommend an alternate solution to removing this barrier?
7. How is this particular business practice affected in a manual or electronic environment?

These 7 questions guided the work groups as they documented the practices shared by the stakeholders, identified barriers and their legal sources, and developed solutions and implementation plans to reduce or eliminate the barriers to exchanging electronic health information.

The following steps were taken to identify the legal drivers of the information-sharing business practices:

1. The LWG reviewed the scenarios.

2. The LWG researched North Carolina and federal laws relevant to the type of HIE addressed in the scenario.

3. Then the LWG was given access to the results of the assessment sessions. The group reviewed the interviewees' current practices and policies.

4. The LWG identified the gaps between the relevant laws and the current understanding and application of those laws by the various health organizations.

5. The LWG recommended solutions to the legal barriers presented. The group also advised the SWG on proposed policy solutions that either may pose a liability risk to stakeholders or may conflict with state or federal law.

The SWG chairman, Dave Kirby, developed a work plan that included weekly goals to allow members first to understand the problems and issues and then to formulate candidate solution outlines. These steps were followed by an opportunity to add commentary to the solution outlines that then would be analyzed and commented upon by other project participants. This last element took the form of written subgroup reports. The work plan allowed each subgroup to work simultaneously. This design feature reduced the risk of missing the large project milestones because of a single group's delay. The plan called for the subgroups to vet the various solutions and was structured to allow every viewpoint to be represented in the interim and final reports, together with group views of the applicability of each solution offered. This part of the plan anticipated an environment in which there was sufficient risk to each barrier and sufficient urgency in finding solutions, and it anticipated an environment in which each offered solution would be pressed forward in some venue in North Carolina at least to the point field testing. The project manager correlated and consolidated the various inputs and developed the report.

The HISPC Domains of Privacy and Security

RTI supplied the state project team with a set of domains to consider as the SWG and LWG considered solutions. This set of domains is derived from standard information security principles. Domains 1–6 are relevant to organizations that have implemented electronic health information systems. Because of the limited amount of implemented technology among the interviewees, most of the barriers that were identified centered around Domains 7–9. The 9 domains are as follows:

1. user and entity authentication to verify that persons or entities seeking access to electronic personal health information are who they claim to be;

2. information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information;

3. patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises;

4. information transmission security or exchange protocols (encryption, etc) for information that is being exchanged over an electronic communications network;

5. information protections so that electronic personal health information cannot be improperly modified;

6. information audits that record and monitor the activity of health information systems;

7. administrative or physical security safeguards required to implement a comprehensive security platform for health IT;

8. state law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged; and

9. information use and disclosure policies that arise as health care entities share clinical health information electronically.

Summary of Relevant Findings

The VWG and LWG analyzed the responses from the stakeholders and identified policy, legal, and technological barriers that prevented or delayed the exchange of health information.

BR_1. Range within organizations of misinterpretation or misapplication of laws or regulations

Interviewees consistently shared that, unless they were required to share the information, they would rather "protect" it for fear of being held liable for breaching an individual's right to privacy. The VWG, LWG, and SWG found that most of the misinterpretation or misapplication of laws, regulations, or organizational policies stemmed from a lack of awareness that the law, regulation, or policy existed, or from a lack of training that was meaningful to the organization or individual.

BR_2. Lack of business incentives to exchange information

Clinicians who were interviewed feared that engaging in an interoperable HIE such as a RHIO could cause them to lose patients to other providers. They also were interested in the benefits of EHRs but were not sure how such large monetary investments in technology could benefit their patients or their practices. The SWG believed that the lack of health information technology (HIT) adoption and HIE is due to providers' perception that HIT lacks value, to the lack of funding to implement such technology, and to a lack of incentives for sharing information with other entities.

BR_3. Lack of policy standardization across entities

The interviewees and members of the LWG and SWG observed an overall lack of policy standards within their own organizations and industry-wide. Consents and authorizations to treat patients and to release patient information vary from entity to entity. Differing legal and political philosophies cause differing approaches to the application of laws and regulations, resulting in differing information-sharing practices among health care stakeholders.

BR_4. Lack of security standardization across entities

The VWG, LWG, and SWG concurred that the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules laid the foundation for entities to develop privacy and security programs. However, if the goal is to implement an interoperable health information network in order to securely exchange electronic health information, then specific, formal security standards should be identified and adopted by the health care community.

BR_5. Lack of interoperability between processes and technology

The health care system is fragmented. Before technology is implemented, a review of the industry's health care processes should be undertaken to identify where the breakdowns in interoperability occur and whether the appropriate remedies for each breakdown are ones of process or of technology.

BR_6. Lack of workable technology

The adoption of effective HIT is critical to an interoperable nationwide health information network.

BR_7. Conflicting or outdated federal or state laws or regulations

Current privacy laws were appropriately implemented to protect the confidentiality of information. As electronic information exchange increases, however, laws focusing on the confidentiality, protection, and disposal of information contained in paper format should be reviewed and updated to reflect the new medium of exchange.

Consumer Empowerment Barriers

The following barriers were not derived from stakeholder responses. They have been identified by the SWG and LWG in response to the ONC's objectives of ensuring that consumer concerns are identified and represented as the development and implementation of the Nationwide Health Information Network ensues.

BR_8a. Lack of consumer understanding or awareness of the benefits of HIT, which leads to a lack of consumer input into the policy and technology that support health information exchange

To ensure usability, systems designers should engage consumers and seek regular input on how consumers can use HIT and exchange to improve their health.

BR_8b. Lack of definition of consumer empowerment and lack of methodology for including consumers in policy and systems design

Clarifying the term *consumer empowerment* in relation to the ONC's strategy would assist policy makers and technology experts in developing policy and technology that empowers and improves the lives of consumers. If consumer empowerment includes consumers' ability to manage the access to their health information, then application software would be required to include such features.

Subgroup 1 (Patient Care Direct Treatment Scenarios): Stakeholders

1. Patient Care A (Emergency Transfer)
2. Patient Care B (Substance Abuse)
3. Patient Care C (Access Security)
4. Patient Care D (HIV and Genetics)

Twenty-nine respondents participated in the assessment sessions for Subgroup 1, the patient care scenarios. The respondents included physician groups, clinicians, hospital health information managers and nursing staff, researchers, hospital privacy officials, and health law attorneys (who responded on behalf of their hospital clients or were familiar with hospital operational issues). The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario (for an overview of the barriers identified by the VWG and LWG and the domains addressed, see the tables below).

Number of Stakeholders' Responses Regarding Barriers, by Patient Care Scenario

	Scenario Number			
Barrier	**1**	**2**	**3**	**4**
BR_1. Misinterpretation of laws		29		
BR_2. Lack of business incentives				
BR_3. Lack of policy				
BR_4. Lack of security		29		
BR_5. Lack of interoperability	29			
BR_6. Lack of technology	29			
BR_7. Conflicting laws		29	29	29

Privacy and Security Domains Addressed, by Patient Care Scenario

	Scenario Number			
Domain	**1**	**2**	**3**	**4**
1. Authentication	X		X	
2. Authorization	X	X	X	X
3. Identity Matching	X	X	X	X
4. Transmission	X	X	X	X
5. Integrity			X	
6. Event Audit			X	X
7. Safeguards			X	
8. Data Classification	X			X
9. Policies	X	X	X	X

Subgroup 2 (Payment Scenarios): Stakeholders

5. Payment (EHR Access)
9. Pharmacy Benefit A (Mail Order)
10. Pharmacy Benefit B (Claims Savings)

Nine individuals responded to Scenario 5. They included staff members from the payer community who specialize in case management, as well as health and corporate law. Respondents to Scenario 7 included HIPAA privacy officials, physician group administrators, health information professionals, clinicians, and research professionals. No pharmacy benefit managers (PBMs) responded to the invitation to participate in the assessment regarding Scenarios 9 and 10. The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario (for an overview of the barriers identified by the VWG and LWG and the domains addressed, see the tables below).

Number of Stakeholders' Responses Regarding Barriers, by Payer/PBM Scenario

	Scenario Number		
Barrier	**5**	**9**	**10**
BR_1. Misinterpretation of laws			
BR_2. Lack of business incentives			
BR_3. Lack of policy			
BR_4. Lack of security			
BR_5. Lack of interoperability			
BR_6. Lack of technology	9		
BR_7. Conflicting laws	9		

Privacy and Security Domains Addressed, by Payer/PBM Scenario

	Scenario Number			
Domain	**5**	**7**	**9**	**10**
1. Authentication	X			
2. Authorization	X			X
3. Identity Matching	X		X	
4. Transmission	X		X	
5. Integrity		X		X
6. Event Audit	X	X		
7. Safeguards				
8. Data Classification		X	X	
9. Policies	X	X	X	X

Subgroup 3 (Secondary-Use Scenarios): Stakeholders

Subgroup 3 scenarios were based on the uses and disclosures of health information for the purposes of conducting health care operations, marketing, or work-related activities that have no impact on direct patient care. The 27 respondents for Scenario 6 included individuals representing clinicians, hospitals, health plans, public health agencies, laboratories, pharmacies, professional associations, and academic medical centers. The 32 respondents for Scenario 8 included individuals representing clinicians, hospitals, payers, public health agencies, laboratories, pharmacies, law enforcement, professional associations, academic medical centers, county government, and the legal community. The 5 respondents for Scenarios 11 and 12 (Group 3, Health Care Marketing and Operations) included marketing professionals that specialized in hospital wellness programs from the hospital, payer, and disease management communities. The 26 respondents for Scenario 14 (employee health information) included human resources professionals and employees from self-insured employers, payers, academic medical centers, hospitals, and group-practice administrators. The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario (for an overview of the barriers identified by the VWG and LWG and the domains addressed, see the tables below).

Subgroup 4 (Government, Public Health, and Safety Scenarios): Stakeholders

13. Bioterrorism Event (Anthrax Spread)
15. Public Health A (Active TB Carrier)
16. Public Health B (Newborn Screening)
17. Public Health C (Homeless Shelters)
18. Health Oversight (Legal Compliance)

Number of Stakeholders' Responses Regarding Barriers, by Secondary Use of Health Information Scenario

	Scenario Number					
Barrier	**6**	**7**	**8**	**11**	**12**	**14**
BR_1. Misinterpretation of laws				5	5	26
BR_2. Lack of business incentives		1				
BR_3. Lack of policy	27					
BR_4. Lack of security	27					
BR_5. Lack of interoperability		1				
BR_6. Lack of technology		1				26
BR_7. Conflicting laws	27		32			26

Privacy and Security Domains Addressed, by Secondary Use of Health Information Scenario

	Scenario Number					
Domain	**6**	**7**	**8**	**11**	**12**	**14**
1. Authentication		X		X		
2. Authorization	X		X	X	X	X
3. Identity Matching	X	X			X	
4. Transmission	X	X		X	X	X
5. Integrity	X	X				X
6. Event Audit	X			X		X
7. Safeguards	X					X
8. Data Classification		X	X	X	X	
9. Policies	X	X	X	X	X	X

Respondents to scenarios 13 and 15–18 (Group 4, Public Health and State Government) included North Carolina state government employees representing public health agencies, substance abuse, mental health, emergency management, laboratories, hospitals, clinicians, medical and public health schools, health information management, and disaster and homeland security professionals. There were no participants from drug treatment centers or homeless shelters. The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario (for an overview of the barriers identified by the VWG and LWG and the domains addressed, see the tables below).

Number of Stakeholders' Responses Regarding Barriers, by State Government and Public Health Scenario

	Scenario Number				
Barrier	**13**	**15**	**16**	**17**	**18**
BR_1. Misinterpretation of laws					
BR_2. Lack of business incentives					
BR_3. Lack of policy	19				
BR_4. Lack of security					
BR_5. Lack of interoperability	19	11			8
BR_6. Lack of technology		11			8
BR_7. Conflicting laws			12	14	

Privacy and Security Domains Addressed, by State Government and Public Health Scenario

	Scenario Number				
Domain	**13**	**15**	**16**	**17**	**18**
1. Authentication			X		X
2. Authorization	X	X	X	X	X
3. Identity Matching	X	X	X	X	X
4. Transmission		X	X	X	X
5. Integrity	X	X	X		X
6. Event Audit	X			X	X
7. Safeguards					X
8. Data Classification	X	X	X	X	X
9. Policies	X	X	X	X	X

Summary of Solutions

The VWG, LWG, and SWG analyzed the barriers to information exchange and proposed solutions to reduce or eliminate barriers that delay or prevent stakeholders from exchanging health information with each other. The solutions are organized by characterizing the scope of the practice of information exchange to which each solution would apply. They are additionally organized according to the organizations that indicate the traits of various solutions related to historical issues of electronic health data exchange.

In the state report, each proposed solution conveys further detail on the barrier that it addresses; the rationale for the particular proposed solution; an alternate solution, if applicable; to whom the proposed solution applies; and potential barriers to implementing the proposed solution. The Implementation Plan report will contain detailed information on

the anticipated length of implementation, potential resources for it, and steps for implementing each solution.

The following proposed solutions are not ranked in any particular order of priority:

- SOL_1. Establish a pilot project with adequate funding to explore the concept of the Person-Oriented HIE.
- SOL_2. Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information.
- SOL_2a. Implement security standards to address the complexity and ambiguity surrounding the safeguarding of health information.
- SOL_3. Implement sound business models to incentivize potential information-sharing partners to participate in community-based HIE.
- SOL_4. Encourage greater collaboration between policy makers and subject matter and technical experts to adopt HIE requirements.
- SOL_5. Explore the dependencies between the business processes and their technical components for the purpose of interoperability.
- SOL_6. Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.
- SOL_7. Amend conflicting federal or state laws.
- SOL_8. Develop programs to increase awareness about the risks, benefits, and effects of HIT among a cross-section of consumers.

Conclusions and Next Steps

The HISPC project has convened a core group of North Carolina consumers and health care professionals from varying segments of the health care system. The discussions within the VWG, LWG, SWG, and steering committee, as well as Consumer Advisory Council meetings, have generated interest in further exploring the identified barriers and implementing the proposed solutions. The Implementation Plan report will propose high-level steps for interested stakeholders to consider as they plan for the implementation of the proposed solutions.

The implementation challenge for the North Carolina stakeholders is that there is no executive-level mandate or financial sponsorship to spur implementation of the proposed solutions at this time. Therefore, the next steps for the North Carolina stakeholders will be to

1. raise awareness about the expected benefits of adopting HIT,
2. develop programs that foster the growth of HIT thought leadership,

3. educate and engage the North Carolina General Assembly in the promotion of HIT, and

4. cultivate the Consumer Advisory Council.

To participate in the continuing efforts or to view more information on the state project team efforts, see the NCHICA site at http://www.nchica.org/NCHISPC/intro.htm.

OHIO—SUMMARY

The purpose of the final Assessment of Variations and Analysis of Solutions report is to provide, for each state, a high-level summary of (1) variations discerned in the analysis, (2) the status of current health information technology (HIT) initiatives, and (3) the most significant interim solutions proposed in their individual reports.

Adoption of HIT is on an upward trend in Ohio. The state created the Third Frontier initiative, a publicly funded effort to promote development and dissemination of cutting-edge information technology across the state. Ohio is also working toward statewide coordination of health information exchange (HIE) through public forums hosted by the Health Policy Institute of Ohio (HPIO) and through developing regional health information organizations across the state, two of which are currently actively engaged in HIE. HPIO has also coordinated the creation of an HIT/HIE Roadmap for Ohio, with input from a broad stakeholder base, and is providing state legislators and the new governor's office with recommendations for moving forward with statewide coordination and monitoring of HIE efforts. Regional projects include the following:

- The Center for Healthy Communities in Dayton has implemented an electronically shared, community-wide health record based on the continuity of care record (CCR) standard.
- HealthBridge in Cincinnati is an Internet portal through which more than 100 entities supply, and thousands of users retrieve, laboratory reports in a standardized format.
- The Community Health Alliance of Northwest Ohio in Toledo is an infrastructure that includes a neutral community-centric data processing center and a highly leveraged service center.
- Several Cleveland hospitals are working with one of the Nationwide Health Information Network prototype demonstration projects to develop HIE architecture.
- Cleveland-Akron area Northeast Ohio Regional Health Information Organization (NEORHIO) was created in 2006.
- In central Ohio, the major health systems and the business community, represented by some of the area's major employers, are working together to evaluate the feasibility of starting a local Community Health Network (CHN). The first phases of this evaluation will be focused on creating a self-sustaining business models centered on key initial deliverables provided by such a network, and on finding appropriate funding sources for the formation of a regional health information organization to implement and support the CHN.
- The Appalachian Regional Informatics Consortium has been funded by the National Library of Medicine to create a sustainable and replicable model for advanced integrated information management systems for rural health care in Appalachian Ohio.

Ohio presented its solutions within 6 major groupings: (1) establishing national standards for HIE; (2) creating a universal patient identifier (or method); (3) standardizing role-based system access models; (4) securing proactive financial support for the adoption of HIT; (5) addressing handling of sensitive health information; and (6) focusing the purpose of adoption of technology on improved quality of care. Recommended solutions included the following:

- Identify and use a unique identifier for patient identification, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included. In the future, accurate identification of patients should be through biometrics.
- Develop role-based access standards and standard audit trails documenting by time and date stamp and source all read and write access to protected health information.
- Standardize the application of *medical need to know* and *minimum necessary*.
- Take responsibility on the state level for developing the basic infrastructure to support HIE.
- Establish a mechanism to allow electronic implementation of patient consent, and adjust current laws and practices accordingly.
- Adopt CCR standard or other generally accepted standard for determining type of data routinely exchanged with regard to Medicaid, mental health, substance abuse, and other diseases (such as HIV/AIDS).
- Establish requirements that any publicly funded projects must conform to national standards including CCR.
- Integrate Employee Retirement Income Security Act, Family Educational Rights and Privacy Act, and Health Insurance Portability and Accountability Act regulations.
- Educate consumers in order to articulate the perceived value of HIE against the perceived risk of privacy and security breaches in an electronic system.

OKLAHOMA—SUMMARY

Widespread use of electronic health records should provide a means of improving quality of care, lowering health care costs, and preventing medical errors. Improved patient care and additional cost savings can be realized through seamless electronic communication of clinical information between institutions in a private and secure fashion.

The federal government funded a project known as the Health Information Security and Privacy Collaboration in 33 states and a single territory to assess how organizational business policies and practices and state laws regarding privacy and security affect health information exchange (HIE) on a national level.

Oklahoma was selected to participate and was awarded an 11-month contract by RTI International. Oklahoma's information will be combined with other states', with the eventual goal to develop a nationwide electronic health information network. Therefore, this initiative is significantly advancing Oklahoma's understanding of how to use electronic information exchange to transform the health care system without compromising the privacy and security of sensitive medical information.

The Oklahoma state project team was charged with examining business policies and state laws related to privacy and security of HIE. The project offered opportunities for health care professionals throughout Oklahoma to participate in identifying privacy and security practices relating to HIE.

As the first step in the process, the Variation Work Group, comprising a diverse and multidisciplinary group of stakeholders from across the state, identified the organizational-level business practices of HIE as it relates to security and privacy. RTI structured the collection of this data through the use of 18 scenarios and 9 domains of privacy and security. The business practices collected were grouped in primary categories of authentication, contractual agreements, consent for service, data management, release of information, transfer of patient health information, and security. The Legal Work Group met concurrently to determine whether or not a legal driver was one rationale for the business practice.

The research from this project reflects that there is significant variation in business practices across organizations in Oklahoma. Although most business practices supported state and federal privacy and security laws, many entities had business practices in place that were more restrictive than the law required. This conservative approach was deemed to be based on a general lack of understanding or misinterpretation of what personal health information can be released and under what conditions, and of the security requirements for the information.

Other underlying causes were discussed and documented to further enhance the solution and implementation phases of the project, including liability, cost, and standardization. It was determined that the top 7 barriers impeding interoperable health information exchange in the State of Oklahoma were as follows:

- overly restrictive interpretations of Health Insurance Portability and Accountability Act (HIPAA) and other privacy and security laws,
- lack of knowledge of HIPAA and other privacy and security laws,
- varied and manual transfer of protected health information,
- concerns over liability for information released,
- cost of implementing and maintaining electronic systems,
- lack of standards, and
- patient consent/release of information.

The next step in the process ushered in the Solutions Work Group (SWG) and Implementation Planning Work Group (IPWG). The SWG worked hand-in-hand with the IPWG to identify a number of solutions to move the state closer to interoperability. The solutions were vetted, and 3 solutions were considered to have the greatest impact and feasibility for completion within the next 12 to 18 months:

- developing an office of HIE,
- creating a universal authorization-to-release form, and
- researching and proposing a patient identification system.

This project has helped lay the groundwork for public and private partnerships as the state begins to move toward electronic HIE. The IPWG is developing implementation plans to support the top 3 state solutions and is addressing how Oklahoma can continue to move toward interoperable HIE.

OREGON—SUMMARY

The electronic exchange of health information holds the potential to revolutionize health care in many ways, including improved quality, cost-efficiencies, enhanced patient-consumer engagement, and greater continuity of care. Within the broad arena of health information exchange (HIE), the Oregon Health Information Security and Privacy Collaboration (HISPC) is exploring the issues of privacy and security. Governor Ted Kulongoski appointed a HISPC steering committee with a breadth of expertise and depth of commitment to accomplish the work of the project. The project is a collaboration of the Oregon Health Care Quality Corporation and the Office for Oregon Health Policy and Research.

Vision

- Oregonians' health information is available to them and their health care providers anytime, anywhere it is needed.
- Oregonians' health information is private and secure at all times and across all transactions.
- Oregonians' health information is used to assure that personal and population-based health care is safe, effective, and efficient.

Values

The goal of this effort is to keep Oregonians' health information private and secure. The following values frame Oregon's policy for assuring the privacy and security of electronic health information:

- trust
- privacy
- autonomy
- feasibility
- balance
- portability
- equality
- transparency
- public accountability

Critical Issues

The health care environment is changing: electronic health records are replacing paper records and health information is increasingly being exchanged electronically. The electronic exchange of information has the potential to revolutionize health care through improved quality, cost-efficiencies, enhanced patient-consumer engagement, and greater continuity of care. While the technology to do so is emerging, there is still a great deal of work to be done to allow for a smooth transition into this new world.

To function in this new environment, trust relationships must be built between individuals and organizations involved in health care or the handling of health information. Multiple high-profile inappropriate disclosures have heightened consumer concern for the privacy and security of their electronic health information. The need to protect individuals' privacy must be balanced with the need to share individuals' health information so that care is safe, effective, and efficient. Achievement of this balance between potentially conflicting values necessitates an approach that includes an enhanced role for the individual in determining the flow of his or her health information.

Recommended Solutions

***Consumer protection*.** Adopt the Markle Foundation's *Connecting for Health* principles regarding the individual and his or her health information as guiding principles for consumer protection:

- Individuals should be guaranteed access to their own health information.
- Individuals should be able to access their personally identifiable health information conveniently and affordably.
- Individuals should have control over whether and how their personally identifiable health information is shared.
- Individuals should know how their personally identifiable health information may be used and who has access to it.
- Systems for HIE must protect the integrity, security, and confidentiality of an individual's information.
- The governance and administration of HIE networks should be transparent and publicly accountable.

***Provider identification*.** A coordinated approach to identifying, authenticating, and authorizing providers should exist.

***Patient identification*.** A coordinated approach to identifying, authenticating, and authorizing patients should exist.

***Public engagement*.** An educated and engaged Oregon population regarding health information privacy rights and expectations should emerge.

***Specially protected information*.** An examination should be undertaken of state laws that define specially protected health information to determine the appropriateness of the protections and the feasibility of implementing these protections in an electronic environment.

***Medical identity theft*.** An examination should be made of state laws regarding identity theft to determine if medical identity theft is appropriately and adequately addressed.

***Technical assistance*.** Support should be offered to organizations for comprehensive adoption of appropriate privacy and security practices for the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state law compliance.

***Noncovered entities*.** Legal privacy and security requirements not covered by HIPAA should emerge for entities handling personal health information.

***Secondary use*.** An examination should be undertaken of current practices for secondary use of data, in order to determine an acceptable balance between ensuring that personal health information is protected, and making de-identified data available for appropriate use.

***Enforcement*.** Legislative or regulatory measures should emerge to address inappropriate disclosures and mitigate potential harmful effects of personal health information disclosure.

***State leadership*.** In order to ensure that evolving electronic health information systems adequately protect the privacy and security of individuals, Oregon's state leadership must coordinate the identified solutions.

PUERTO RICO—SUMMARY

The Puerto Rico Health Department (PRHD) is committed to the development and implementation of health information systems that facilitate health information exchange. It was awarded a grant by RTI International to participate in the Health Information Security and Privacy Collaboration (HISPC) project. Its participation in this project allows the PRHD to develop a descriptive analysis of the public and private business practices, policies, and state laws affecting electronic health information exchange, and to then propose feasible solutions and implementation plans that promote and allow for interoperability in health information exchange, in accordance with relevant security and privacy regulations within the territory.

The descriptive analysis of variations and review of proposed solutions toward interoperability, at the center of the current stage of the HISPC project, are significant because they make it possible to juxtapose the description and evaluation of existing practices, policies, and laws with the proposed solutions to barriers that unnecessarily impede information exchange. The dual focus of the report will serve as a resource in future efforts to promote interoperability, ensure security, and protect the privacy of patients and consumers in Puerto Rico. It can also assist in the development of corrective measures that will help bring local practices, policies, and laws in line with federal and international initiatives.

Puerto Rico's HISPC project is managed by a local project management team (PMT), which is composed of the director of HIPAA and External Affairs, a member of the Legal Advisor's Office of the PRHD, and two consulting teams. The HIPSC steering committee acts as the decision-making body for the course of this project. It is tasked with overseeing and finalizing deliverable reports. These reports will serve as the basis for identifying and taking steps toward the realization of increased and more efficient health information interoperability.

In order to understand the dynamics of health information exchange on the island, the HIPSC project's steering committee and the PMT convened a Variations Work Group (VWG) and Legal Work Group (LWG). These groups have been composed primarily of health care professionals and health care providers from both the public and private sectors. The VWG met regularly to identify variation within business practices and to document institutional policies that characterize the exchange of protected health information in Puerto Rico. It identified practices and policies that address the privacy and security of personal health information exchange for 18 different scenarios that RTI provided to the PMT. In addition, the PMT determined whether each business practice that it identified in discussions with stakeholders is best classified as barrier, as aid, or as neutral with respect to

interoperability. The LWG was tasked with the identification of legal drivers, underlying laws, regulations, court cases, and legal barriers to interoperability.

The information about business practices provided and assessed in the Puerto Rico report was gathered through 3 different methods: in discussions that took place in meetings of the VWG, from a survey distributed to health care providers, and through interviews held with particular stakeholders. The PMT collected information from these 3 sources and compiled it in a Microsoft Excel spreadsheet.

The report, the final assessment report for the security and privacy project, describes variation in institutional and business practices, policies, and laws and provides critical observations on the 18 scenarios provided. It does so by discussing the following 9 domains:

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

RHODE ISLAND—SUMMARY

Overview

Deliverable 5, Final Assessment of Variation in Organizational-Level Business Practices and Analysis of Privacy and Security Solutions, was prepared by the Rhode Island Department of Health and its stakeholder participants in the Rhode Island Health Information Security and Privacy Collaboration (HISPC) in preparation for satisfaction of a contractual requirement to RTI International. The purpose of the document was to present the final findings from a statewide process of documenting and assessing variations in current health information exchange (HIE) practices, policies, and laws and to present a final account of proposed solutions derived from this assessment. These solutions are intended to advance strong privacy and security protections to enable interoperable electronic HIE in Rhode Island. Using the final Assessment and Analysis of Solutions, this report has also established the basis for the final Implementation Plan report to be submitted at the conclusion of the HISPC project.

Rhode Island has leveraged the governance and committee structure of its ongoing HIE network initiative for the HISPC project. Leadership, managers, staff, and committees served as the core state project team to develop and refine HISPC work products. The Assessment of Variation included 27 health services and government agency stakeholder groups in an analysis of their respective HIE practices as applicable to a set of RTI-defined scenarios. This process included the transcription of stakeholder meeting details and the subsequent development of concise statements describing relevant HIE, or business practices. Each practice has been correlated to a primary privacy and security domain—there are 9 domains that are of particular interest to RTI. Privacy and security domains found to be of significance in the assessment of variation have served as important factors in the analysis of solutions presented in this report.

The report is divided into 5 major sections:

1. Background and Purpose
2. Assessment of Variation
3. Analysis of Solutions
4. Conclusions and Next Steps
5. Appendices

Descriptive details on all notable business practices referenced in this report, including both those classified as barriers to HIE and those deemed "effective" practices, are listed in Appendix A of the report. All final business practice details have been rendered anonymous

(except with regard to state government agencies), documented, and maintained in the RTI online assessment tool. The entire set of business practices is available to stakeholders on request from the HISPC project manager.

Final Assessment of Variation

A specific process was used to identify and document 153 distinct HIE practices for participating organizations across the state. These business practices have been validated by the participating stakeholders to ensure that they are complete and accurate. A professional legal review and analysis of applicable state and federal laws has been used as a benchmark for practice classification. Practices have been classified as "barriers" or "neutral" to HIE, depending on the policies and laws that drive them. Policies and practices supportive of privacy protections that were stricter than prevailing laws were not considered barriers unless they placed an undue constraint on permissible exchanges of information. The classification criteria and other details of the assessment are included in Section 2.

It is notable that most practices (73%) documented through the assessment process are related to HIE for treatment and payment purposes. Thirty-two of 153 HIE practices (21%) were identified as barriers to HIE, and 91% of these barriers occur in the treatment and payment purposes category. It is also important to note that, as a percentage of the total number of barriers grouped by domain, the greatest proportion of barriers (53%) occur in the "Information Use and Disclosure Policies" domain. This percentage is followed by 16% of the total number of barriers in each of two other key domains: "Information Authorization and Access Controls" and "State Law Restrictions About Information Types and Classes." These findings confirm the need for improvements in these domains and are consistent with current efforts by Rhode Island stakeholders to use patient-driven authorization practices to improve privacy protections in the emerging Rhode Island HIE.

Critical observations, issues, and implications for solutions that arose from the assessment of variation can be summarized as follows:

1. Variations in practices to obtain patient authorization for the release of information span the full range of drivers, including state and federal laws, organizational policies, and distinct business practices. Above all other issues, authorization practices and their integral relationship to health information use and disclosure is the major area of focus for improving privacy and security protections in the exchange of health information in Rhode Island. While special classes of information may require different authorization practices under the law, and these practices may present some degree of constraint on HIE, the variability in authorization practices for "general" health information points to a broader set of issues that reflect fundamental differences in consumer, provider, and organizational views on patient privacy protections.

2. Restrictive policies prohibiting consulting physicians access to hospital-based electronic health records (EHRs) tend to have technical origins that increase the risk of unauthorized or incidental disclosure. Solutions should be pursued, including

appropriate identification policies, authentication mechanisms, and education and training to promote physician adoption and use of a range of electronic health information systems, including the statewide HIE network.

3. In general, in cases in which outside entities, such as health plans, are given access to an organization's EHR for legitimate utilization review or payment authorization purposes, solutions should focus on consistent implementation of clear and reasonable disclosure parameters, auditing policies, and the assurance of auditable access control technology for health plan and other EHR users. The need for strong access control and audit policies will be especially important to establish consumer trust in an HIE network.

4. Upholding strong human subjects review and institutional review board procedures will be essential to preserve and protect health information for research purposes. As the Rhode Island community contemplates permitted uses of health information accessed through the Rhode Island HIE, it is clear that an important area of focus will be to ensure privacy and confidentiality protections and strong governance and oversight of data use decisions, such as research.

5. Secure interorganizational clinical communication methods and networks appear to be a high-value application to support patient-provider communication and treatment and payment practices; however, these methods and technologies are not widely deployed.

6. Current Rhode Island law provides for the use of digital signatures or other electronic authorization methods in place of written signatures; however, this capability is not used in routine practice. Solutions to enable broad use of digital signatures must be embraced to enable the proliferation of electronic HIE independent of paper-based documentation methods.

7. In the interest of promoting consistent, readily understandable policies and procedures for the protection of special classes of information, a legal solution will be required to put sexually transmitted disease information on par with other protected classes of information, such as substance abuse, mental health, HIV/AIDS, and genetic testing.

8. As Rhode Island proceeds with the development and implementation of a statewide HIE system, several legal issues must be resolved to enable a high-value, highly used system to evolve.

9. Federal Family Educational Rights and Privacy Act (FERPA) regulations pose strict consent requirements on exchanges of school health information and can have a significant impact on public health programs, especially child health, welfare, vaccine-preventable disease prevention, and communicable diseases.

10. Solutions to HIE barriers must take into account the incremental adoption of electronic health information systems.

Final Analysis of Solutions

The final solutions described in Rhode Island's report include a priority set of fundamental building blocks intended to enable interoperable electronic HIE. The HISPC steering

committee provided insightful direction as to the prioritization of approaches to implementing responsible privacy and security protections. This guidance included positioning all solutions relative to essential areas of capability development required to accomplish private, secure HIE through the Rhode Island HIE network. The resultant solution set addresses policies, methods, and standards in 4 areas: (1) protecting data confidentiality and integrity, including authorization and access controls; (2) ensuring reliable authentication of network users and patients; (3) matching and merging patient records in the Rhode Island HIE; and (4) auditing capability for monitoring access to the network.

Section 3 provides a detailed account of the process for solution identification, development, prioritization, and determination of feasibility. In addition, detailed profiles are included for the 4 final solutions that have been advanced to the implementation planning stage. While Rhode Island's strategy is to first develop statewide HIE capacity, this report describes preliminary planning discussions between Rhode Island and Connecticut regarding the potential for interstate HIEs involving each state's HIE network. These discussions are initially focused around 3 areas:

- quantitative and qualitative assessment of the value of cross-state health care business to articulate the need for interoperable HIE;
- comprehensive policy assessment of consent requirements in both Connecticut and Rhode Island HIE environments and determination of an acceptable approach to consent management in cross-state exchanges; and
- assessment of information infrastructure and consideration of using applicable Integrating the Healthcare Enterprise interoperability profiles to establish the framework for seamlessly passing core health information for patient care coordination between Connecticut and Rhode Island HIE networks.

Rhode Island offers the following national-level recommendations as preliminary ideas derived from the work to date:

1. The US Department of Health and Human Services, Office of the National Coordinator (ONC), should strongly consider the recommendations advanced through the January 23, 2007, report issued by the Foundation of Research and Education of the American Health Information Management Association, Development of State Level Health Information Exchange Initiatives Final Report: Extension Tasks, with special attention to Task #1: Relationship of State-Level HIE to Federal/Other HIT Activities. On the basis of the findings of this study, ONC and the US Department of Health and Human Services should implement a series of strategic and tactical actions that maintain coordination and open communication among state and federal HIE initiatives.

2. There should be review and clarification of specific laws and regulatory guidance in the context of emerging state and regional HIE organizations. Key areas of focus should include (1) clarification of 42 U.S.C. § 290dd-2 regarding the breadth of applicability of federal funding status on the release of alcohol and substance abuse

treatment records; (2) review of Clinical Laboratory Improvement Amendments regulations in light of HIE organizations that endeavor to provide electronic laboratory reporting services; and (3) review of FERPA, 34 C.F.R. pt. 99, restrictions on the authorized release of school health records, in light of HIE organizations that endeavor to support public health planning and disease surveillance activities.

Conclusion

The report describes how the HISPC privacy and security initiative has contributed to advancement of the work required to ensure that the Rhode Island HIE network demonstrates responsible privacy and security protections for the electronic exchange of health information. As for next steps, Rhode Island will continue in an active state of development and implementation of its statewide network after the HISPC project ends:

- The Rhode Island strategy is to direct and coordinate specific privacy and security implementation plans through the structure of its ongoing HIE initiative.
- All privacy and security policies and technical approaches for the Rhode Island HIE will be tested in a narrowly defined pilot project, with additional data types and data-sharing partners to be added as resources permit.
- Future evolution of the Rhode Island HIE will preserve the fundamental principles and guidelines articulated and approved by Rhode Island stakeholders.
- Once statewide HIE capability is achieved, consistent privacy and security protections will be intact in the statewide network environment and be capable of being extended to authorized interstate exchanges.

UTAH—SUMMARY

Beginning in July of 2006, the Utah Network for Electronic Public Health Information, Privacy and Security, project began collecting data from Utah's health care community regarding health information exchange (HIE) business practices, policies, and state laws. The state's report is the third in a series that documents the efforts of the project work groups to identify constraints on appropriate exchanges of health information, privacy or security risks, and solutions that balance privacy and security and facilitate appropriate exchanges of health information while ensuring patient rights.

Utah's health care industry is in transition from a paper to an electronic environment and requires policies supportive of a phased migration. The findings refine and expand on the two previous interim reports, Assessment of Variations and Interim Solutions, which were offered by the Variations Work Group (VWG) and Solutions Work Group. The report consists of 6 major sections:

1. Background and Purpose
2. Assessment of Variation
3. Summary of Key Findings from Assessment of Variations
4. Review of State Solution Identification and Selection Process
5. Analysis of State Proposed Solutions
6. National-Level Recommendations

The data for this report was collected from a volunteer nonrandom sample of Utah health care stakeholders that were determined to have knowledge or engage in business practices relevant to each scenario. Care was taken to include diverse representatives from (urban and rural areas; different-sized organizations; profit, nonprofit, and independent organizations) Utah to provide a comprehensive report of interoperability privacy and security.

The VWG met to determine which of the 154 business practices collected served as a barrier, without judgment, to HIE within the state. From these meetings, 3 key findings emerged:

1. Health care providers obtained patient authorization to disclose health information for all situations except emergency situations.
2. Variations existed regarding the methods used to transmit protected health information (PHI), with fax transmission being the most common. Variation further existed with regard to beliefs about, and understanding of transmission security.

3. Rules and statutes varied with regard to PHI, and, as a result, entities implemented business practices according to a variety of legislative guidelines. These guidelines primarily included either the Health Insurance Portability and Accountability Act or 42 C.F.R. pt. 2.

The Legal Work Group determined that a few business practices were driven by state statute. Utah privacy or tort law was cited more often as a constraint, in that organizational practices were defensive measures put in place to protect against tort litigation.

E-Health in Utah is quickly becoming accepted as a means to improve health care, lower costs, and promote healthier communities. It is clear that continuing to move e-Health forward requires development of infrastructure capacity to support interoperability. Utah's history of public-private partnership demonstrates a commitment to open-market solutions. While the proposed solutions represent only one network, a strategic planning effort must include all players in the health care industry, as well as vendors and other entities that bring vital resources to the table. An open dialogue is required to gain common understanding if participants are to succeed in communicating with other agencies and organizations while maintaining privacy and security.

The solutions presented in the report are intended to preserve essential privacy and security protections, establishing a foundation for consumer trust with a patient's bill of rights, and moving forward electronic connectivity to permit appropriate exchange of health information.

VERMONT—SUMMARY

The Vermont state project team did not include an executive summary.

WASHINGTON—SUMMARY

As part of the US Department of Health and Human Services's health information technology plan for creating a nationwide health information network, 34 state/territory-level Health Information Security and Privacy Collaboration (HISPC) projects completed 10 months of work in April 2007 to address privacy and security issues affecting interoperable electronic health information exchange (HIE). In April 2006, Governor Christine Gregoire's office designated Qualis Health, a not-for-profit health care quality improvement organization based in Seattle, to lead the HISPC project in Washington State.

In June 2006, Qualis Health entered into contract with RTI International to facilitate diverse groups of volunteer experts in HIE to participate in a series of work groups tasked to

- assess organizational-level business policies, practices, and state laws that affect HIE;
- identify and propose practical solutions that protect privacy and security of health information and permit interoperable HIE; and
- develop plans to implement solutions in the state and, if applicable, at the federal level.

The state's final report embodies the collective expertise and opinions of more than 100 Washington State volunteer experts in HIE and related privacy and security issues, representing more than organizations and interest groups. As part of RTI's prescriptive HISPC process, work groups identified over 360 business practices and policies related to current practice for HIE between entities. The majority of business practices collected during that process related to information use and disclosure policies, information authorization and access controls, and information transmission security or exchange protocols.[8]

A group of 12 volunteer experts, called the Variations Work Group, assessed these business practices and labeled them as either a barrier[9] to electronic HIE, an aid to it, or neutral toward it. These findings served as the starting place for the Solutions Work Group, whose task was to draft solutions to remove unnecessary barriers to electronic HIE. The Solutions Work Group participants recognized early on that the lack of generally accepted minimum privacy and security standards related to electronic HIE was a major barrier to widespread adoption of effective business practices that promote increased interoperability. They developed a process-based set of 3 solutions with the goal to protect privacy and security of

[8]All Washington State HISPC reports, Interim Assessment of Variations (containing all identified business practices), Interim Analysis of Solutions, and Interim Implementation Plan, are available on the Qualis Health website: www.qualishealth.org/HISPC.

[9]RTI defined a *barrier* to health information exchange as a practice, policy, or law that impedes, prohibits, or imposes conditions on HIE (without judgment regarding the degree of appropriateness for the barrier in question).

health information while reducing or eliminating unnecessary or inappropriate privacy and security obstacles to electronic HIE:

1. Develop a *minimum set* of operational and technical requirements, together with related policies and procedures, that participants in HIE need to have in place to achieve secure transmission of personal health data and protect patient privacy. This "Privacy and Security Core Solution Set" addresses 4 domains:
   - User and Entity Authentication
   - Authorization and Access Control
   - Use and Disclosure Policy
   - Transmission Security
2. Work with public and private stakeholders throughout Washington State to develop and implement provider and consumer incentives to adopt the Privacy and Security Core Solution Set.
3. Establish an administrative body to develop, administer, and promote use of the Privacy and Security Core Solution Set. The administrative body will focus on the following major activities:
   - Oversee development of consistent policies, procedures, and standards for implementing the Privacy and Security Core Solution Set.
   - Assist the Washington State legislature, the Governor's Office, and state regulatory agencies to establish incentives for stakeholder adoption and implementation of the Privacy and Security Core Solutions Set.
   - Develop education, training, and collaborative activities that promote stakeholder implementation of the Privacy and Security Core Solution Set.
   - Develop interpretive guidance to resolve confusion about current state and federal privacy and security laws to assist in reducing risk and liability concerns that are currently obstacles to participation and investment in electronic information exchange.
   - Work with the Washington State legislature, the Governor's Office, and state regulatory agencies to amend current laws that are barriers to HIE and create new laws to address emerging security and privacy needs.
   - Coordinate with corresponding parties in other states to promote consistency in privacy and security solutions related to multistate HIE.

The Implementation Planning Work Group expanded upon this work by documenting practical approaches and actionable steps for implementing the recommended process-based solutions. The implementation plan as outlined in the report focuses on establishing an administrative body that carries with it the authority to develop and promote the Privacy and Security Core Solution Set. The implementation plan does not advocate a specific governing structure, but instead describes optional structures that could be employed. Options include models such as the Health Insurance Portability and Accountability Act standards process and the electronic health records certification process currently used by the Office of the National Coordinator of Health Information Technology. The concept is to

establish an administrative body that develops and recommends privacy and security policies, procedures, and standards to a governmentally authorized entity that, in turn, adopts them by regulation or other official action. As stakeholders invest in electronic HIE systems, they would have incentives to comply with the privacy and security standards, such as the assurance that their risk and liability will be moderated through some form of "safe harbors" treatment, or other types of incentive.

The ideal implementation plan would call for establishing the administrative body first, with development of the standards and incentives under its umbrella. However, implementation in the State of Washington must adapt to the political and practical realities of the state HIE environment. The Washington Health Information Infrastructure Advisory Board (HIIAB), an authoritative body convened by law in 2005, delivered a report and recommendations for a state health information infrastructure to the legislature in December 2006. Legislative action on the HIIAB recommendations is expected in the near future, and the next phase is expected to commence summer 2007. The HISPC recommendations generally complement and support implementation of the HIIAB recommendations, and HIIAB implementation in turn may provide support for or facilitate adoption of the HISPC recommendations. One of the recommendations of the HIIAB is the formation of a nongovernmental, nonprofit entity to play a key role in Washington State health information infrastructure development. If this recommendation is followed, such an entity might logically be the sponsoring entity for the administrative body described in this report.

Establishing the specific details of the structure and sponsorship of the HISPC's administrative body is problematic at this time because it depends upon resolution of the HIIAB's implementation and the legislature's funding priorities. Therefore, a key recommendation in this report is implementation of a HISPC "bridge" strategy. This bridge strategy will include the establishment of a "light" administrative structure to provide for communications, meetings, and the like, and one or two work groups to continue development of solutions and so maintain momentum and trust in the process. If and when the HIIAB's recommendations are implemented, it will then be feasible to pursue a more formal linked arrangement between HIIAB and HISPC. If the HIIAB recommendations are not implemented or discussions make it clear that a linked arrangement is not feasible, then the longer-term strategy is to establish the HISPC administrative body independently or through another existing sponsor.

The momentum and interest generated by the HISPC in Washington State has been considerable. The potential to improve the quality of patient care in a more cost-effective manner through widespread use of electronic HIE, and the state government's leadership role in promoting the adoption of health information technologies, make the privacy and security solutions and implementation plans described within this report timely, relevant, and achievable.

WEST VIRGINIA—SUMMARY

Project Background

In May 2006, the West Virginia Medical Institute was awarded a contract by RTI International to participate in the National Health Information Security and Privacy Collaboration project. This project is part of a national effort of the US Department of Health and Human Services's Office of the National Coordinator for Health Information Technology, the Agency for Healthcare Research and Quality, and the National Governors Association. West Virginia is one of 34 states and US territories to receive a contract for this work. The goal of this project is to assess variations in business practices related to the private and secure exchange of health information among various stakeholders, analyze the legal basis for these practices, propose solutions for barriers found to interfere with health information exchange and develop plans to implement the proposed solutions. This work has been accomplished by 4 groups focusing on each of these goals: the Variations Work Group (VWG); the Legal Work Group (LWG); the Implementation Plan Work Group (IPWG); and the Solutions Work Group (SWG).

Methodology

To begin, the state project team invited individuals representing 17 stakeholder groups to join the VWG. Through a series of meetings, teleconferences, and focus groups, the VWG analyzed a collection of 18 scenarios addressing the use and disclosure of health information. The work group members described business practices and policies that would be followed by their respective organizations in responding to each scenario. These business practices encompassed 9 domains of security and privacy, including whether or not a given domain would be considered a barrier to interoperability. These business practices were collected with use of an assessment tool provided by RTI.

The LWG identified applicable privacy and security laws, regulations, court cases, and other legal sources governing the exchange of health information. Then they analyzed each business practice for legal barriers and mapped those barriers to applicable federal and state legal drivers. This information was added to the assessment tool. The completed assessment tool was distributed to a wider group of stakeholders for additional comment, and the data was then uploaded to the RTI project portal.

The SWG and IPWG elected to merge their groups and treat the solution search and implementation planning as a single process. The chairpersons believed that discussions generating solutions would lead immediately to proposed implementation plans as they attempted to prioritize solutions and that it would be more efficient and productive to permit such discussions to reach their integral conclusions. These groups worked together to arrive at a set of actionable tasks designed to address each of the key solutions identified in West

Virginia's Interim Solutions report. The IPWG tested the reality of many of the recommendations contained in this report by soliciting public, provider, and consumer response through a series of public meetings that were convened around the state. Comments and recommendations acquired through these exchanges assisted the IPWG in framing many of its final recommendations.

The implementation plan presents a practical and detailed framework including activities that will lead to the fulfillment of the project's short- and long-term objectives. The plan identifies the stakeholders that will be tasked with implementation responsibilities necessary to ensure that West Virginia is able to sustain an ongoing process leading toward the successful, safe, and secure exchange of health information electronically.

Summary of Critical Observations

Key issues and findings of the work groups include the following:

- To achieve the goal of improving the overall quality of health care, an electronic health record (EHR) system must maximize the ability of health care providers to share information for treatment purposes. West Virginia policy makers should consider the express adoption of the national Health Insurance Portability and Accountability Act standard as it applies to all patients.

- Current West Virginia law does not allow e-prescribing and is unworkable in the context of an interoperable EHR network. The law should be modified to allow e-prescribing in some regulated form.

- Some West Virginia stakeholders have already begun the transition from a paper system to an EHR network. The West Virginia Health Information Network must take a leadership role in developing and implementing standardized business practices for stakeholders to utilize upon joining the statewide interoperable EHR network.

- The achievement of increased administrative efficiency for the payment and reimbursement of health services is another promise of EHRs. Again, it is recommended that West Virginia closely follow the national standard established by HIPAA, which allows health information to be disclosed for payment purposes without prior patient authorization or consent.

- A statewide interoperable EHR network will accumulate vast amounts of data. West Virginia policy makers must ensure that the statewide network properly balances public access to such data with patient privacy.

Barriers to health information exchange generally fall into 3 broad categories: inconsistent state and federal laws, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice. The state project team believes that each of these barriers can be addressed through the development of creative legislative, regulatory, technical, administrative, and educational solutions.

WISCONSIN—SUMMARY

In November 2005, by Exec. Order No. 129, Governor Doyle created the eHealth Care Quality and Patient Safety Board (eHealth Board). The goal of the eHealth Board is to have 100% adoption of electronic health records systems and the appropriate exchange of health information from these systems within 5 years. The eHealth Board was charged with developing a roadmap for achieving this goal.

The eHealth Board submitted the Wisconsin eHealth Action Plan to the governor in December 2006. This plan addresses the following challenges:

- ensuring that health information is available at the point of care for all patients;
- reducing medical errors and avoiding duplicative medical procedures;
- improving coordination of care between hospitals, physicians, and other health professionals;
- furthering health care research; and
- providing consumers with their health information to encourage greater participation in their health care decisions.

A key concern identified in the eHealth Action Plan is the requirement to exchange health information electronically in a way that is secure and protects a patient's privacy. In March 2006, the Department of Health and Family Services applied for the Health Information Security and Privacy Collaboration (HISPC) contract on behalf of the eHealth Board; the resulting effort is referred to as the *Wisconsin Security and Privacy Project.* Wisconsin was one of 34 states and territories awarded a contract to assess the security and privacy issues related to eHealth.

The Wisconsin Security and Privacy Project began in the fall of 2006 with the formation of 4 work groups: Variations, Legal, Solutions, and Implementation. In the development of the 4 work groups required by this project, Wisconsin was fortunate to have 52 individuals who volunteered their time and represented advocates, clinics, consumers, corrections, health care organizations, health care providers, health care quality organizations, hospitals, industry, laboratories, pharmacies, professional associations, public health, schools, payers, and state government.

Assessment of Variation

As required by the HISPC contract, the first group convened in this process was the Variations Work Group. The Variations Work Group was charged with reviewing 18 scenarios developed by RTI International to identify current business practices related to health

information exchange (HIE), as well as the driver for each business practice. The work group discussed variations in business practices between the responding stakeholders, as well as which business practices posed barriers to HIE. For business practices considered barriers to exchange, the work group discussed which barriers should remain as a privacy protection and which could be reduced or eliminated without removing necessary privacy protections. Staff assisted in the review of the business practices and the determination of which practices related to the domains in information exchange as identified by RTI.

The Legal Work Group was convened shortly after the Variations Work Group to identify the legal drivers of the business practices identified by the Variations Work Group, and it evaluated potential legal barriers to HIE. The Legal Work Group reviewed the 18 scenarios and identified and cited the legal drivers for business practices, as well as all legal barriers associated with the scenarios.

A summary of the barriers documented and analyzed by the Variations and Legal Work Groups follows.

Barriers Driven by Wisconsin Law

Wisconsin statutory requirements that relate to HIE and are more restrictive than federal requirements cause barriers to the exchange of information.

Some of the greatest statutory barriers to HIE are the regulations associated with the treatment of sensitive information, defined as information pertaining to mental health, alcohol and other drug abuse, and developmental disability. The requirements include

- consent for specific types of disclosures (payment and treatment),
- verification of the requestor for this information, and
- the *minimum necessary* rule.

HIV test results are also treated as sensitive information (Wis. Stat. § 252.15), except that they can be disclosed from provider to provider for treatment purposes.

Other barriers driven by Wisconsin law include the following:

- documentation of all disclosures made with or without patient consent, including that defined in Wisconsin Statutes Chapter 146;
- requirements prohibiting redisclosure of health information;
- consent requirements more stringent than federal requirements, such as those for disclosure to the patient's family; and
- required interface between state and federal law requirements.

Barriers Driven by State and Federal Law

Whenever state and federal law do not mirror one another, several barriers to the exchange of information are created. First, one must determine which law controls (state or federal); then, once the controlling law is determined, one must understand the requirements of the controlling law. This makes interstate exchange of information increasingly difficult because other state laws must be understood in order to exchange.

Consent requirements, governed by state and federal law, present the greatest hurdles to HIE. The barriers are caused by

- the process to obtain a consent, including determination of who is able to sign;
- validation of the statutorily required elements of the consent;
- analysis required of state and federal law to determine which law controls; and
- variation in requirements between states.

Although eliminating these consent requirements would reduce the barriers to exchange, federal law 42 C.F.R. pt. 2 requires patient consent to exchange alcohol and other drug abuse information for treatment purposes, unless revision of that federal law occurs.

Other areas where state and federal law differ include

- the *minimum necessary* rule,
- verification of requester, and
- the requirement to provide a Notice of Privacy Practices.

Barriers Driven by Federal Law

In some cases, federal law is more stringent than state law. In all of these cases, both the law and the varying interpretations of the law cause barriers to exchange. The federal requirements identified by the work groups and that pose barriers to exchange include the following:

- verification of the individual requesting the information;
- release of the *minimum necessary* amount of health information for the purposes identified by the individual requesting the information;
- to govern the exchange of information, implementation of business associate agreements that meet the needs of both the covered entity and the vendor;
- the federal Security Rule, which governs the technical security measures to guard against unauthorized access to electronic health information;
- the federal Privacy Rule requirements, including patient rights; and

- regulation of the use of protected health information when the use would not specifically be deemed a disclosure, such as when information is used to perform an internal business function.

Barriers Driven by Policies and Practices

The Variations and Legal Work Groups identified several barriers to HIE that are driven by organizational-level business policies and practices. Most often, variations in policy and practice implementation create barriers to HIE.

Barriers driven by policies and practices include the following:

- consent—varying interpretations of when consent is required for disclosure;
- method of requesting information—varying methods for making requests;
- method of disclosure—varying methods for disclosing information;
- method of retention;
- variability of implementation of the law;
- method for making or responding to a request, such as by phone, by fax, or in writing; and
- sophistication of the technology that an organization is willing to purchase to secure its patients' information.

The final barrier identified by the work groups is technology. In general, current technology used in Wisconsin cannot limit access to relevant parts of the record or to specific records to comply with *minimum necessary* requirements. Furthermore, currently employed technology often cannot specify the type of access (read-only, edit/modify, delete) granted to the user. For those who do not have electronic medical records, the lack of technology creates a barrier to exchange. This issue will not be an easy barrier to overcome, because technology systems are extremely expensive and many providers cannot afford the cost of technology. In addition, the costs related to the *implementation* of technology were also deemed a significant barrier to exchange.

Assessment of Solutions

Solutions Work Group

The Solutions Work Group was charged with the analysis of identified barriers, balancing privacy protections against the need to know, and developing solutions to improve the exchange of health information. The Solutions Work Group included a mix of members from the previous work groups, as well as new members who increased representation in advocacy and policy making, for a total of 35 members. Members represented clinics, hospitals, consumer organizations, law enforcement, health care quality organizations,

industries, pharmacies, professional associations, providers, public health, research, state government, health information vendors, and payers.

The Solutions Work Group reviewed health information barriers caused by variations in organizational-level business practices and relevant state and federal laws as identified by the Legal and Variations Work Groups. The Solutions Work Group followed a complex, creative approach that included a series of small breakout groups and large group discussions to allow active participation from all members, the capture of varied viewpoints, and ultimately the creation of solutions that will improve HIE without compromising necessary patient privacy protections. Through this process, each barrier was analyzed to determine whether it should remain or be reduced or eliminated. Solutions were developed to reduce or eliminate barriers that the group decided should not remain, and they were finally grouped into broader solutions with a greater feasibility of implementation.

Summary

An overview of the proposed solutions is provided below.

Verification of Patient

Currently, health care providers do not use a uniform method to capture standardized criteria to identify a patient (*patient identifiers*).[10, 11] Moreover, there is not a standard method to verify patient identifiers at the time of exchange.[12] This lack of standardization creates significant risks to accurate and timely patient care. Variation in practice also poses a number of challenges to exchanging information in a paper or electronic format. Moving into an electronic world where information is exchanged between electronic health care systems will require standardized collection of patient identifiers, verification of patient identifiers, and accurate matching of identifiers to patient information. Currently, national efforts are under way to develop a set of unique patient identifiers to alleviate these issues.

The solution proposed by the Solutions Work Group addresses current issues with misidentification of patients while positioning Wisconsin to incorporate the national recommendations once they are completed.

The Solutions Work Group proposed the development of a standard set of identifiers, as well as a set of model policies and procedures to ensure appropriate capture and verification of those identifiers. The state project team would maintain an understanding of national efforts to develop a national set of identifiers and would develop policies and procedures that accommodate the national recommendations. This way, Wisconsin's model policies and

[10] *Capture:* The process of collecting patient identifiers from a patient.
[11] *Patient identifiers:* information collected from a patient to assist in the identification of the patient (eg, name, birth date, address).
[12] *Verification:* The process of confirming that patient identifiers are correct.

procedures can be easily revised to incorporate national standards once they are established.

Modification of Wisconsin Statutes Chapter 146 to Mirror HIPAA in Specific Areas

Many of the barriers to HIE result from strict privacy protection requirements in the Wisconsin privacy laws. While some of the restrictions clearly interfere with or prohibit information exchange, others are so complex in their application that they result in wide variation in practices relating to disclosures. Additional barriers are created because the Health Insurance Portability and Accountability Act (HIPAA) creates privacy protections in many of the same areas as Wis. Stat. §§ 146.81–146.84; therefore, application of these laws is complicated because it is difficult to determine which law applies.

Based on a review of the barriers to HIE created by the Wisconsin Statutes Chapter 146, the Solutions Work Group proposed revising these statutes to mirror the language in HIPAA in the following areas:

1. expanding disclosures to family (Wis. Stat. §§ 146.82, 146.83)
2. expanding disclosures to law enforcement
3. modifying redisclosure restrictions (Wis. Stat. § 146.82(2)(b))
4. modifying the requirements for documentation of disclosure (Wis. Stat. §§ 146.82(2)(d), 146.83(3))

The Solutions Work Group determined that these additional restrictions did not significantly improve patient privacy; instead they added to the complexity of HIE, which can result in individuals' not having the information required to diagnose, treat, or care for patients.

Modification of Wis. Stat. § 51.30 to Allow the Exchange of Health Information for Treatment Purposes

Wis. Stat. § 51.30 provides additional protections for health data that contains information related to mental health, developmental disabilities, and alcohol and other drug abuse. These additional protections create barriers to the exchange of information, some of which are arguably necessary privacy protections, while others, it can be argued, deter the exchange of information that could lead to better care. Additional barriers are created because Wis. Stat. § 51.30 is more restrictive than HIPAA regarding the exchange of information protected by this law.

The Solutions Work Group reviewed barriers associated with these restrictions and determined that Wis. Stat. § 51.30 should comport with HIPAA and be revised to allow exchange of information between providers, without patient consent, for treatment purposes. While this change would allow the exchange of information protected by this law,

it would not affect the provider's inability to disclose treatment information without patient consent as protected by 42 C.F.R. pt. 2, the federal statute protecting such information. Consent would still be required to exchange this information.

It should be noted that the majority of the members of the Implementation Work Group further refined the solution and determined that the law should be revised to allow the exchange of information for treatment purposes, but the group did not determine what information should be exchanged freely without consent.

Changes to HIPAA

The Solutions Work Group reviewed all of the barriers associated with the HIPAA Privacy Rule that were identified through the Variations and Legal Work Groups' review of the 18 scenarios. Following discussions of the barriers, the Solutions Work Group proposed the following 3 changes to HIPAA:

- Remove the requirement for a business associate agreement, and instead develop a method to hold business associates accountable for adhering to state and federal privacy requirements.
- Remove the waiver process for research without patient consent, but maintain the institutional review board process requirements.
- Clarify the *minimum necessary* standard by revising the language in HIPAA and developing model policies and procedures to define and clarify the standard.

This proposed solution was not reviewed by the Implementation Work Group, because it was determined that a plan to implement changes to federal law would most efficiently and effectively be created by individuals experienced with national legislative change.

Next Steps

The eHealth Board extends its sincere appreciation to all of the volunteers who dedicated their time to the Security and Privacy Project. The information that has been collected through this process will be valuable as the eHealth Board begins the implementation phase in developing electronic systems and a means to exchange health information electronically.

The recommendations contained in the report represent possible solutions to the challenges identified through the analysis of the 18 scenarios. The recommendations are intended to inform policy discussions but should not be construed as the comprehensive or definitive legislative recommendations of the eHealth Board at this time. The eHealth Board will be using the Security and Privacy Project reports to assess where the proposed solutions fit within the eHealth Board's scope of work for the coming years. Wisconsin is committed to developing the necessary policies and procedures to ensure the adoption of health information technology and exchange throughout Wisconsin in an effort to ensure quality of care and patient safety.

WYOMING—SUMMARY

Wyoming is one of 34 states and territories awarded a subcontract with the US Department of Health and Human Services, Agency for Healthcare Research and Quality, through RTI International, to address privacy and security policy questions affecting the interoperable exchange of electronic health information among the numerous organizations that make up the health care community. The Health Information Security and Privacy Collaboration (HISPC) project is designed to identify variations in privacy and security practices and laws affecting electronic information exchange; develop best practices and propose solutions to address identified challenges; and increase expertise about health information privacy and security protection in communities. The Wyoming HISPC project will also produce an implementation plan for the solutions identified in the analysis.

The state report represents the final assessment of variations in Wyoming's organizational-level business policies and practices, and identification of significant issues and barriers in the exchange of health information. This report also describes the solutions identified by stakeholders to address those issues associated with health information exchange. Project staff met with a broad spectrum of stakeholders throughout Wyoming, all of whom helped assess Wyoming's processes for exchanging health information. While Wyoming has very few examples of electronic health records (EHRs), stakeholders have identified significant issues regarding health information exchange in general and barriers to an electronic health information system in particular.

When the issue of an electronic medical records system is discussed, the central concern of Wyoming stakeholders is *cost*. Many of the small hospitals and clinics simply cannot afford the infrastructure needed to implement an EHR, and organizations that can afford EHRs are hesitant to purchase them. *Interoperability* and *technology obsolescence* are key concerns. Many stakeholders have concerns about investing in systems that will be outdated in a few years or unable to communicate with other systems.

Another major issue uncovered is the *regional* nature of Wyoming's health care. Because more than 30% of Wyoming's health care is delivered outside the state, many stakeholders view any type of statewide EHR as inadequate. However, these regional concerns must be balanced with a strong state-centered attitude identified among many stakeholders. Stakeholders fear the security and privacy of health care information may be compromised if the current system, which relies heavily on personally and professionally knowing the individual on the other end of the phone, is replaced with an impersonal, electronic system.

The legal and practical issues surrounding redisclosure of medical records, whether paper or electronic, were also a major topic of discussion. Confusion and misinformation on the subject has led many stakeholders to release information much more conservatively than

legally required, for fear of potential lawsuits involving wrongful disclosure. Furthermore, this culture of fear leads many health care professionals to release incomplete medical records, because they believe they cannot redisclose another provider's records. There is particular confusion regarding mental health and substance abuse records, the relationship between health care providers and law enforcement, the legal procedure for blood alcohol testing, and other similar issues.

APPENDIX B
DESCRIPTIONS OF HEALTH INFORMATION EXCHANGE DEVELOPMENT AND HEALTH INFORMATION TECHNOLOGY ADOPTION BY STATE

Table B-1. Descriptions of Health Information Exchange (HIE) Development and Health Information Technology (HIT) Adoption by State

State	Description of HIT Development by State
Alaska	**HIE Overview:** Alaska health care leaders and members of the Alaska Telehealth Advisory Council formed the Alaska Regional Health Information Organization (AK RHIO), now known as Alaska ChartLink, which has been working with the support of the Alaska governor's office on the Health Information Security and Privacy Collaboration (HISPC). The HISPC Core Project Team includes members from the State of Alaska, the Alaska Electronic Health Record Alliance, Alaska Native Tribal Health Consortium, physicians, health care consumers, and legal and meeting facilitation contractors. An initiative is under way to assist private practice clinicians in selecting and implementing office-based electronic health records (EHRs). **HIT Adoption:** Environment is described as favorable, but adoption is not widespread. Many physicians using electronic billing systems, but only 25% have a functional EHR system.
Arkansas	**HIE Overview:** In the past 5 years the state began to identify and gather resources to put into place infrastructure to support linkage between underdeveloped rural areas (still predominant in Arkansas) and more highly developed urban areas. This linkage enhancement program is currently facilitated by 2 key organizations: the Arkansas Rural Health Collaboration and the Arkansas Foundation for Medical Care. Both have identified expansion of HIT infrastructure to underserved nonurban areas and health care facilities as critical to adequately support creation of a true statewide HIT network. **HIT Adoption:** HIT is described as *nascent*. Conditions favorable for adoption vary geographically: central and northwestern regions have experienced workforce and other resources to support IT and HIT; eastern and southeastern regions lack these resources.
Arizona	**HIE Overview:** Arizona's Health-e Connection, the statewide HIE initiative, which was created by executive order in 2005, is now an active nonprofit organization. Its implementation teams are achieving first-year deliverables. A 5-year Roadmap has been completed. Arizona's first regional health information organization (RHIO), the Southern Arizona Health Information Exchange (SAHIE), has been organized; it developed a business plan and is now developing an implementation plan. Also, the Arizona Health Care Cost Containment System, the State's Medicaid Agency, is organizing an HIE within the Medicaid system. **HIT Adoption:** Large practices, hospitals, laboratories, and pharmacies have adopted various forms of HIT. Estimates of HIT adoption among small practices range from 15% to 19%.
California	**HIE Overview:** CalRHIO, California's statewide HIE organization, has been incorporated as a nonprofit organization. Two important tasks have been completed: a Strategic Plan and a vendor selection process to facilitate and operate the statewide HIE. **HIT Adoption:** CalRHIO conducts a quarterly inventory of HIT activities in the state. In summer 2006, CalRHIO identified 16 HIE initiatives at various stages of development.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
Colorado	**HIE Overview:** CORHIO, Colorado's Regional Health Information Organization is the nonprofit state-level HIE initiative. It incorporates the efforts of the state's Agency for Healthcare Research and Quality (AHRQ) state and regional demonstration project (the Colorado Health Information Exchange, or COHIE) and aims to build a statewide federated interoperable HIE environment. COHIE provides technical expertise and leads prototype development for connecting divergent platforms and products. CORHIO will ultimately support several types of statewide data exchange, including point of care, secure clinical and administrative messaging, and population data exchange. CORHIO's incorporation and building of major components for point of care exchange are under way during 2007. **HIT Adoption:** HIT adoption is most advanced along the eastern slope of the Rocky Mountains and in several small western and southwestern cities. The report estimates 10% to 15% of Colorado physicians, mostly in small practices, have implemented EHRs.
Connecticut	**HIE Overview:** Connecticut has established the eHealth Connecticut, the state's acting RHIO. eHealth Connecticut has outlined plans for 5 major projects over the next 2 years, including plans to (1) educate, collaborate, and adopt standards; (2) implement HIE and an e-prescribing project; (3) share HIE information (starting with lab, medication information, and emergency department); (4) implement statewide database of clinical quality and cost information for public reporting; and (5) develop an incentive program for providers to spur the adoption of HIT. In addition, the University of Connecticut Center for Public Health and Health Policy is developing the Connecticut Health Information Network, which uses a federated database architecture in a secure networked environment. **HIT Adoption:** A recent survey by eHealth Connecticut indicated 17% of physician offices have implemented EHRs; 25% plan to implement EHR in the near future; and 58% could connect electronically to hospitals.
Florida	**HIE Overview:** In 2004, the governor established the Health Information Infrastructure Advisory Board to advise the state on the development of the Florida Health Information Network (FHIN), an integrated vision intended to guide local health information networks toward interoperability. FHIN will become a network of networks connecting RHIOs and other health networks. Florida has provided funding to spur communities to develop local HIEs. Several HIEs/RHIOs have been established. **HIT Adoption:** Florida has participated in the national movement to improve the quality of health care and health outcomes by focusing on how HIT can enhance communications at every level of the health care delivery system.
Illinois	**HIE Overview:** The state's HIE efforts are in an early stage of development. The Illinois Electronics Health Records Taskforce (EHRTF) recently submitted its final report to the Illinois General Assembly. One of the task force's recommendations calls for the creation of a not-for-profit organization, the Illinois Health Information Network (ILHIN), to establish a state-level HIE. The Illinois Department of Public Health would form a public-private partnership with ILHIN to advance EHR and HIE initiatives within the state if task force recommendations are enacted.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
	HIT Adoption: Another key recommendation of the task force is for the department/ILHIN public-private partnership to create an initiative to foster the adoption of EHR systems by health care organizations and the development of regional HIEs.
Indiana	**HIE Overview:** The Indiana Network for Patient Care is described as the oldest, largest, and most robust clinical HIE in the nation and is at the forefront of HIT. Programs involve public health and scientific researchers as an integral part of the exchange.
	HIT Adoption: The state has a well-developed clinical messaging service, has a medication history service, and recently launched an e-prescribing service. The exchange is implementing a service to provide clinical and claims data to support community quality initiatives of payers and providers. While much of central Indiana is quite advanced, other areas are at varying stages of HIE or EHR adoption (or both).
Iowa	**HIE Overview:** The state is in the beginning stages of HIT implementation and interoperability. Several statewide initiatives are under way to encourage the use of HIT and HIE to improve health care quality, including the Iowa HIT Initiative, the Iowa Electronic Medical Records Task Force, and Iowa Medicaid Electronic Records System, which is conducting a pilot to (1) implement portions of an EHR within the Iowa Medicaid program and (2) test electronic sharing of the information with the outside health care community.
	HIT Adoption: Most large health care provider organizations in the state are currently implementing EHRs. But the smaller and rural providers are noticeably falling behind.
Kansas	**HIE Overview:** The Kansas Health Care Cost Containment Commission is overseeing development of a plan for the state's HIE initiative. A steering committee has been formed, and a roadmap identifying foundational, organizational, and environmental actions was recently completed.
	HIT Adoption: Citing earlier research, a 2006 report by the eHealth Initiative Foundation noted that 21% of physician offices used electronic clinical information of some kind; 51% of hospitals reported electronic access to laboratory results; 34% reported having electronic imaging systems; and 24% reported use of electronic medication administration records. Kansas providers have significant concerns about financing, availability of technical support, and rural high-speed Internet access.
Kentucky	**HIE Overview:** In 2005, the state passed a law authorizing the establishment of the Kentucky e-Health Network. A board was created and charged with overseeing the development of this statewide, interoperable network. The State e-Health Action Plan, a comprehensive strategy to achieve the goals of the Kentucky e-Health Network was completed in April 2007.
	HIT Adoption: An initial assessment of the maturity of Kentucky's e-Health efforts showed that the state has few mature local e-health projects; HIT adoption rates are low; and the state has a number of health care markets, with some of the largest ones crossing state lines; Few are large enough, however, to sustain a RHIO or local e-health initiative. There is a clear need for a statewide e-health development and coordinating structure.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
Louisiana	**HIE Overview:** In Louisiana, the federal, state, and local governments are actively partnering with private health and human services organizations to design and develop several RHIOs, EHRs, disease registries, and interoperability projects. At least 14 major efforts are currently under way in the state, including the National Coordinator for Health Information Technology–funded Louisiana Health Information Exchange (LaHIE). The state is also participating in the Gulf Coast Health Information Technology Task Force. More recently, Louisiana has been undertaking a major Healthcare Redesign Project, of which HIT and HIE are a central component. Currently the state is aligning the LaHIE with the new Redesign Project. **HIT Adoption:** The report describes HIT development as moderate. Several large, private multisite systems effectively connect thousands of providers electronically through their proprietary closed networks, and Blue Cross Blue Shield (BCBS) provides beneficiaries access to claims data via the Internet. Most providers—especially those in rural areas or in solo practice—do not have access to electronic health information, and most consumers do not yet fully benefit from HIT and HIE.
Maine	**HIE Overview:** Maine's statewide initiative to integrate clinical information started in 2004 with a feasibility study, followed by planning and development stages that culminated in 2006 with the establishment of HealthInfoNet as an independent, nonprofit organization. HealthInfoNet is charged with overseeing the development of the statewide electronic clinical information-sharing network. A state strategic plan was completed, and, more recently, a vendor selection process was also completed. Maine's statewide HIE project has continued planning and developing to address system governance, technical system requirements, and consumer engagement while stressing stakeholder involvement and financial support. **HIT Adoption:** In addition to Maine's statewide HIE, there are many organizations with highly advanced HIT development and deployments. Integrated delivery networks (IDNs) have integration between providers, hospitals, labs, mental health system, and public health agencies. Two of the state's larger IDNs are beginning integration of their EHRs. The largest health system in the state has deployed a regional picture-archiving and communication system that will provide computed radiology services for half the population of the state.
Massachusetts	**HIE Overview:** Health information electronic data exchange is in several stages of development. The state has several HIE/HIT initiatives under way, including MA-SHARE and the Massachusetts e-Health Collaborative (MAEHC). The MA-SHARE has been operating as the state RHIO, with several projects under way. In the private sector, pilot projects have also helped develop organizational, contractual, policy, and relationship building blocks for future HIE. Other private-sector HIE projects are designed for ongoing growth, scalability, and business sustainability. In the public sector, the Executive Offices of Health and Human Services (EOHHS), has created a Web portal intended to provide a single access point to all EOHHS initiatives for consumers, providers, legislators, and researchers. **HIT Adoption:** MAEHC is leading the charge toward adoption of HIT and EHRs in clinical practices and communities. It has received $50 million commitment from BCBS of Massachusetts to fund its demonstration project phase.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
Michigan	**HIE Overview:** Michigan has experienced significant progress in the development and deployment of regional HIEs. There are several efforts under way in various parts of the state, most of them started in the last 2 to 3 years and currently in planning or early implementation stages. In addition, the Michigan Health Information Network recently completed its Conduit to Care strategic planning report, identifying the mission, goals, principles, and short-term and long-term steps for the state HIE initiative. The legislature also passed a law creating the Health Information Technology Commission and appropriating $9.5 million to support regional HIE projects. **HIT Adoption**: Like most other states, large Michigan health care organizations have implemented or are in the process of implementing EHRs. Most of the smaller organizations and rural health care providers have not. Recently, the state issued requests for proposals to support HIT investment.
Minnesota	**HIE Overview:** In 2004 the Minnesota e-Health Initiative was established as a private-public collaboration to accelerate the use of HIT in Minnesota. The advisory committee of this initiative is responsible for recommendations to implement a statewide interoperable HIE, including estimates of necessary resources and standards for administrative data exchange, clinical support programs, patient privacy requirements, and maintenance of the security and confidentiality of patient data. **HIT Adoption:** Minnesota's e-Health Initiative reported that in 2006 close to 20% of hospitals in the state have fully implemented EHRs, 5% were testing, and 57% were in partial implementation stage. Among clinics, about 17% have implemented, 29% are currently in progress, and close to 30% are planning to implement in the next 2 years. All others are not currently implementing and do not have plans to do so at this point.
Mississippi	**HIE Overview:** There are silos of HIE activity with possibly some crossover but no coordinated statewide activity. No centralized entity has existed in Mississippi to oversee the implementation of a secure, integrated, interoperable health information network and infrastructure. In March 2007 the governor issued an executive order creating the Mississippi Health Information Infrastructure Task Force, charged with developing an overall strategy for the statewide adoption and use of HIT and HIE. There are 24 regional or community exchange activities under way. The state is also participating in the Southern Governors Association Gulf Coast Health IT Task Force. **HIT Adoption:** No information available.
New Hampshire	**HIE Overview:** The report describes an excellent foundation for HIE/HIT with programs across the state. The New Hampshire Citizens Health Initiative convened in 2006, the second "NH Connect for Health" summit. A roadmap is being developed under the auspices of the University of New Hampshire and New Hampshire Citizens Health Initiative, to define a strategy for governance, sustainability, clinical use, technical approach, and privacy and security of the state's HIE.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
	HIT Adoption: Many health care organizations in New Hampshire have implemented varying degrees of HIT that serve as the foundation for the state to build a regional HIE infrastructure. Among them, Capital Regional Health Care's Centricity EMR (electronic medical record) project, has been adopted by all of the state's community health centers. In addition to several grants and projects, many state hospitals have some form of EHR system. A survey conducted by the New Hampshire Hospital Association of members indicated that most hospitals have adopted HIT for patient accounts, inventory and supply management, pharmacy management, and patient records. The most often cited reason for not expanding IT into other areas of hospital systems was the substantial initial investment of operating capital required.
New Jersey	**HIE Overview:** Last year, the New Jersey Hospital Association (NJHA) convened an EHR/EMR Task Force that recommended an extensive business plan and feasibility study. In December 2006 NJHA and BCBS commissioned a more comprehensive feasibility study and plan for the development of a statewide HIE.
	HIT Adoption: HIT efforts were initiated 14 years ago with The Healthcare Information Networks Technology Study (1994). These efforts have included legal and regulatory actions to set a framework for providers, trade groups, and state entities to explore cross-industry collaboration and dynamic tactical partnerships to further the goals and promises of Health Insurance Portability and Accountability Act administrative simplification and EHR. Other efforts include a National Provider Identification education, enumeration, and rollout project. More than 200 stakeholders have expressed an interest in working on projects associated with the creation of a RHIO and EHR development.
New Mexico	**HIE Overview:** Efforts to develop an HIE network have been under way for 2 years, led by the New Mexico Health Information Collaborative, a community-based initiative funded by AHRQ, community partners, and the New Mexico State Legislature. The basic technical architecture has been built. Three major network architecture elements are in place: a patient index or medical record locator; an infrastructure for transmitting HIE; and a mechanism to exchange clinical messages electronically and securely. Demonstrations are under way in Taos, New Mexico, to implement the exchange.
	HIT Adoption: Large health systems in and around Albuquerque are in the process of implementing EHR systems, and some small cities and towns have adopted EHR. However, the majority of practices, especially small ones, continue to be paper based. The basic technical architecture has been built, and demonstrations are under way to implement the exchange.
New York	**HIE Overview:** There are a number of HIE efforts under way in the state. The state Department of Health convened the HIT Stakeholders Group Planning Committee to develop recommendations on mission, goals, and structure for the statewide HIE initiative. The New York e-Health Collaborative (NYeC) was recently established as a nonprofit organization to develop principles and priorities for the state's HIT strategy; serve as a resource for existing RHIOs and a focal point for communication and education; assess emerging issues and address challenges to interoperability; and support ongoing monitoring and accountability of health IT projects. The next step is to develop a roadmap and strategic plan.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
	HIT Adoption: The state has secured and made available significant financial resources to promote the adoption of HIT and the development of infrastructure that promotes HIE, including the Health Care Efficiency and Affordability Law for New Yorkers (HEAL-NY) Capital Grant Program, a multiphase, $1 billion initiative to reconfigure the State's health care delivery system and improve health care quality and efficiency. Two of the 4 phases are dedicated to providing investments in regional health IT initiatives. HEAL-NY has provided over $52 million to 26 regional health care networks to support the development of clinical information exchange projects, the creation of e-prescribing capabilities, and the use of EHR systems. Public-private partnerships provide strategic development and evaluation for emerging HIE projects.
North Carolina	**HIE Overview:** Several HIT initiatives are under way to automate medication, laboratory, and radiology data; establish an automated surveillance system for adverse drug events; create an emergency department data repository; and implement an electronic version of prenatal medical records. Communities in the Research Triangle, North Carolina, and Rockingham County, North Carolina–Danville, Virginia, areas are engaged in the prototype of a Nationwide Health Information Network. Various health care stakeholders are discussing and taking action to create and participate in RHIOs.
	HIT Adoption: Like other states, North Carolina has seen a significant level of adoption of EHRs among large health care provider organizations in the major cities and a limited number of implementations in rural and smaller provider organizations and clinics
Ohio	**HIE Overview:** The state is working toward statewide coordination of HIE through public forums hosted by the Health Policy Institute of Ohio (HPIO) and through the development of RHIOs across the state, 2 of which are currently actively engaged in HIE. HPIO has also coordinated the creation of a statewide HIT/HIE Roadmap for Ohio with input from a broad stakeholder base and is providing state legislators and the new governor's office with recommendations for moving forward with statewide coordination and monitoring of HIE efforts. The Roadmap was issued in December 2006.
	HIT Adoption: HIT adoption is in an upward trend. Among large hospital systems, most are in the process of implementing enterprise solutions for HIT; none is fully implemented. All of these organizations expect that their vendor will provide an interoperable solution. While some physician practices, large and small, have adopted EHRs, other physician practices may have practice management systems that lack EHRs. Ohio's physicians see the benefit of EHRs, but generally perceive the cost of such systems as prohibitive. Many hospital-affiliated physicians expect their hospital to provide them with an office-based hospital system EHR or expect that the hospital will help subsidize implementation of EHRs in their offices to integrate into RHIO systems being implemented statewide.
Oklahoma	**HIE Overview:** Very little health information is exchanged electronically across organizations, other than for billing purposes or within state and federal government. Several HIE implementations are under way within focused areas of exchange. There is, at this time, no central coordinated effort identified.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
	HIT Adoption: Most health care providers maintain paper-based patient records, and transfer of protected health information is conducted via fax, mail, telephone, or courier. Hospital emergency rooms in the metro Oklahoma City area are also working on developing an interoperable electronic health care system.
Oregon	**HIE Overview:** The Oregon Health Care Quality Corporation is currently facilitating an initial planning process for the development of a statewide HIE. A high-level report describing options for action toward HIE was released in November 2006 by the Oregon Business Council. The Council has commissioned a more comprehensive study on the business case, finance, and mobilization for a state HIE demonstration project. **HIT Adoption:** Vast differences in the sophistication and the level of HIT exist. Oregon has a high degree of EHR adoption in numerous communities around the state. A number of health care organizations have not yet engaged in longstanding statewide discussions regarding the appropriate use of technology to exchange health information and often are not adhering to appropriate privacy and security standards. Attempts have been made to engage these providers, but success has been somewhat limited.
Puerto Rico	**HIE Overview:** The Puerto Rico Department of Health has implemented a regional HIE including the University District Hospital, the Pediatrics Hospital, and the Puerto Rico Medical Services Administration, which share a common database and physical medical records. A second regional HIE effort, the Puerto Rico District Hospital (PRDH) Data Warehouse, includes information from the demographic registry, WIC, immunization, public hospital Health Information System and Electronic Medical Record (HIS/EMR), and public insurance claims. The department is also implementing the Puerto Rico Integrated Health System, a statewide Master Patient Index. **HIT Adoption:** Puerto Rico has several private and public HIT initiatives. The PRDH HIS/EMR Project consists of 21 participating public and private primary care facilities and the PRDH to share access to the HIS/EMR provided by PRDH licenses.
Rhode Island	**HIE Overview:** The Rhode Island Health Information Exchange (RI HIE), an initiative of the Rhode Island Quality Institute, is the state's HIE effort. RI HIE is one of the statewide HIEs funded by AHRQ. A state strategic plan and roadmap has been developed, and initial implementation of infrastructure components of the HIE are currently under way. **HIT Adoption:** The report describes a continued predominance of paper- and fax-based methods used to support HIE. Rhode Island is at an intermediate level of health IT development. Current statistics are not readily available, but there are important indicators of growth in the use of electronic HIT solutions: • hospital-based EHRs are increasing, • EHRs in ambulatory settings are slowly gaining interest, • e-prescribing adoption is slowly increasing, and • statewide HIE is under development.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
Utah	**HIE Overview:** Utah Health Information Network (UHIN) is the state's HIE. It currently routes 95% of the state's health care transactions. The state also received one of AHRQ's "State and Regional Demonstrations of Health IT" supporting a community-based effort to design and implement a statewide HIE network. Specific projects are under way to provide electronic sharing of laboratory results from the lab to the doctor, hospital discharge notes from the hospital to the doctor, a patient's medical and medication history from one doctor to another, and e-prescribing. The Utah Department of Health has begun a yearlong planning effort to develop a business plan for the public health system to participate in sharing of clinical information. The Utah Network for Electronic Public Health Information, or the UNIFY project, has the goal of evaluating the potential benefits of sharing information between the clinical care sector and the public health system. **HIT Adoption:** HIT is making great strides. UHIN estimates that 20% of Utah physician offices have adopted EHR systems. Specific projects are under way to provide electronic sharing of laboratory results from the lab to the doctor, hospital discharge notes from the hospital to the doctor, a patient's medical and medication history from one doctor to another, and e-prescribing.
Vermont	**HIE Overview:** The Vermont Information Technology Leaders (VITL), a nonprofit organization created through a state legislative initiative, is responsible for creating a statewide HIT infrastructure and a plan including standards, protocols, and pilot programs. In January 2007, VITL submitted a preliminary plan detailing a shared vision and guiding principles for the development of the final strategy, due July 2007. **HIT Adoption:** Vermont has much HIT activity in both public and private sectors. A 2006 legislative report proposed 26 IT projects among hospitals and health systems, 10 of which may require HIE with external data sources. Ongoing efforts range from the deployment of large multihospital health care information systems, to EMR deployments for hospital-owned physician practices, to medical imaging and archival solutions. HIT is uneven across the state's hospitals; most have plans to upgrade existing technology in 3 to 5 years.
Washington	**HIE Overview:** In 2005 the state legislature passed a bill requiring the development of a state strategy for the adoption and use of interoperable EHRs and health information technologies. A Health Information Infrastructure Advisory Board has been convened to develop the strategy and to make specific recommendations for a state health information interoperability system, including architecture, business model, and governance. The Advisory Board submitted its report to the legislature in December 2006. The report recommended establishing a board to oversee the initiative, secure funding, and move to implementation. The proposed system is expected to make relevant clinical data from a variety of sources available to patients and providers at the point of care, offer a personal health record for patients, and include a query-able data repository to support syndromic surveillance and population-based chronic illness reporting.

(continued)

Table B-1. Descriptions of HIE Development and HIT Adoption by State (continued)

State	Description of HIT Development by State
	HIT Adoption: State government in Washington has taken a leadership role in promoting the adoption of HIT. One point of the governor's 5-Point Strategy for Improving Health Care in Washington focused on making better use of HIT and adopting EHR systems in all hospitals by 2012. HIT development covers the entire range of technological and operational capability. About 75% of the provider community—primarily small physician groups, solo practitioners, and most public health agencies—are currently using paper-based systems. However, several health care organizations employ state-of-the-art clinical, administrative, and medical record management systems and technologies that support secure HIE. Lack of technology available to such a large proportion of caregivers is a significant barrier to electronic data sharing; however, the sophistication and expertise of many health care organizations is a good foundation for development of HIE solutions.
Wisconsin	**HIE Overview:** In 2005 the governor created the eHealth Care Quality and Patient Safety Board, with the goal of 100% adoption of EHRs systems by health care providers and the appropriate exchange of health information from these systems within 5 years. The board submitted the Wisconsin *eHealth Action Plan* to the governor in December 2006. The plan lays out a roadmap to achieve this vision.
	HIT Adoption: Many large health systems are already moving ahead with EHRs and other investments. A 2005 survey of primary care practices reported that 38% of primary care practice sites used an EHR. A 2006 survey of HIT adoption in 30 rural or very small hospitals (22% of all hospitals in the state) concluded that all hospitals had a core Master Patient Index database; 80% had installed electronic pharmacy, lab, or order entry systems; and few hospitals had interface engines, a lack which inhibits information flow inside the hospital and may hinder participation in HIEs.
West Virginia	**HIE Overview:** In 2006 the West Virginia Health Information Network was established by law. The network is overseen by a board of directors. In September 2006, the board approved a roadmap and strategic plan for the implementation of the network, to be completed in April 2008.
	HIT Adoption: The Governor's Task Force on Electronic Health Records and the Regional Health Information Network are expected to facilitate putting critical health care information in the hands of doctors when care is delivered.
Wyoming	**HIE Overview:** The Wyoming Health Information Organization (WyHIO) was established in 2005 as a nonprofit entity charged with developing the health information communication infrastructure in the state to enhance access, quality, safety, and efficiency of health care in Wyoming. WyHIO is currently working on an assessment of HIT adoption in the state.
	HIT Adoption: The report indicates relatively little infrastructure supporting large-scale HIE. Several health care facilities use EHR systems, but attempts to create infrastructure that would support interoperability among these and developing EHR systems have not been successful. A private firm in Laramie is developing an interoperable EHR system. However, most hospitals and medical practitioners in the state have consistently expressed a strong aversion to sharing medical data.

APPENDIX C
LIST OF STAKEHOLDERS

List of Stakeholders

Information technology experts
Health information management professionals
Compliance/risk management professionals
Consumers and consumer organizations
Hospital personnel/ER staff
Human resources personnel
Employers, including self-insured employers
Clinicians
Physician groups
Federal health facilities
Public health departments
Community clinics and health centers
Laboratories
Long-term care facilities and nursing homes
Homecare and Hospice
Medical and public health schools that undertake research
Correctional facilities personnel

APPENDIX D
GLOSSARY OF ACRONYMS

Glossary of Acronyms

ADD	attention deficit disorder
ADHD	attention-deficit/hyperactivity disorder
AHIMA	American Health Information Management Association
AHRQ	Agency for Healthcare Research and Quality
BAA	business associate agreement
CCHIT	Certification Commission for Health Information Technology
CCR	continuity of care record
CDC	Centers for Disease Control and Prevention
CLIA	Clinical Laboratory Improvement Amendment
CMS	Centers for Medicare & Medicaid Services
eHIE	electronic health information exchange
EHR	electronic health record
EMR	electronic medical record
ER	emergency room
ERISA	Employee Retiree Income Security Act
FERPA	Family Educational Rights and Privacy Act
FTP	File Transfer Protocol
HIE	Health Information Exchange
HIIAB	Health Information Infrastructure Advisory Board
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIS	Health Information System
HISPC	Health Information Security and Privacy Collaboration
HIT	Health Information Technology
HITSP	Health Information Technology and Standards Panel
HMO	Health Maintenance Organization
IAS	Interim Analysis of Solutions
IAV	Interim Assessment of Variation (of Business Practices, Policies, and State Law)
IHDS	Integrated Health Delivery System
ILHIN	Illinois Health Information Network
IPWG	Implementation Planning Work Group
IRB	Institutional review board
IT	Information technology
IVR	Interactive Voice Response
LWG	Legal Work Group
NCCUSL	National Conference of Commissioners on Uniform State Laws
NGA	National Governors Association
NHIN	Nationwide Health Information Network
NPI	National Provider Identifier
ONC	Office of the National Coordinator for Health Information Technology

PBM	pharmacy benefit manager
PMO	project management office
PHI	protected health information
PMT	project management team
RHIO	regional health information organization
RLS	record locator service
SRD	state and regional demonstration
SSL	secure sockets layer
SWG	Solutions Work Group
TAP	Technical Advisory Panel
TB	tuberculosis
VPN	virtual private network
VWG	Variations Work Group