

December 20, 2007

# Privacy and Security Solutions for Interoperable Health Information Exchange

## Impact Analysis

Prepared for

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

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

Prepared by

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

Contract Number 290-05-0015  
RTI Project Number 0209825.000.018



RTI Project Number  
0209825.000.018

# Privacy and Security Solutions for Interoperable Health Information Exchange

## Impact Analysis

December 20, 2007

Prepared for

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

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

Prepared by

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

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

# Contents

---

Section	Page
<b>Executive Summary</b>	<b>ES-1</b>
<b>1. Introduction</b>	<b>1-1</b>
1.1 Background.....	1-1
1.2 Methodology.....	1-2
1.3 The Privacy and Security Solutions Project and the Evolving State and Nationwide Landscape of Health IT and Health Information Exchange .....	1-2
1.3.1 Landscape Before the Project .....	1-2
1.3.2 Evolution of the Landscape During the Project .....	1-3
<b>2. Impact Analysis</b>	<b>2-1</b>
2.1 Legislation .....	2-1
2.2 Executive Orders.....	2-10
2.3 Leadership and Governance .....	2-10
2.4 Stakeholder Education and Knowledge .....	2-13
2.5 Development and Sustainability of Health IT/HIE Efforts in the States.....	2-15
<b>3. Collaborative (Cross-State) Outcomes</b>	<b>3-1</b>
3.1 Collaborative Work Groups .....	3-1
3.1.1 Consumer Education and Engagement.....	3-2
3.1.2 Provider Education.....	3-3
3.1.3 Standards Policy Adoption .....	3-3
3.1.4 Harmonizing State Privacy Law.....	3-3
3.1.5 Consent Options, Outcomes, and Best Practices.....	3-4
3.1.6 Consent Data Elements Required for Data Transfer .....	3-4
3.1.7 Interorganizational Agreements.....	3-5
3.2 Other Cross-State Initiatives and Interstate Projects .....	3-5
<b>4. Overview of Individual States/Territories</b>	<b>4-1</b>
4.1 Introduction to the Individual State/Territory Overviews .....	4-1
4.1.1 Alaska .....	4-1
4.1.2 Arizona .....	4-4
4.1.3 Arkansas.....	4-8

4.1.4	California .....	4-11
4.1.5	Colorado .....	4-14
4.1.6	Connecticut .....	4-17
4.1.7	Florida .....	4-22
4.1.8	Illinois .....	4-26
4.1.9	Indiana .....	4-30
4.1.10	Iowa.....	4-33
4.1.11	Kansas .....	4-36
4.1.12	Kentucky.....	4-41
4.1.13	Louisiana .....	4-46
4.1.14	Maine .....	4-49
4.1.15	Massachusetts .....	4-54
4.1.16	Michigan .....	4-57
4.1.17	Minnesota .....	4-60
4.1.18	Mississippi.....	4-64
4.1.19	New Hampshire.....	4-69
4.1.20	New Jersey.....	4-75
4.1.21	New Mexico .....	4-79
4.1.22	New York .....	4-81
4.1.23	North Carolina .....	4-87
4.1.24	Ohio.....	4-91
4.1.25	Oklahoma .....	4-94
4.1.26	Oregon .....	4-98
4.1.27	Puerto Rico.....	4-102
4.1.28	Rhode Island .....	4-104
4.1.29	Utah.....	4-109
4.1.30	Vermont .....	4-112
4.1.31	Washington .....	4-119
4.1.32	West Virginia .....	4-123
4.1.33	Wisconsin.....	4-126
4.1.34	Wyoming .....	4-132
4.2	Impact in Nonparticipating States.....	4-135
<b>5.</b>	<b>Conclusions</b>	<b>5-1</b>
<b>6.</b>	<b>References</b>	<b>6-1</b>
	<b>Appendix A: Glossary of Acronyms</b>	<b>A-1</b>

# Tables

---

<b>Number</b>		<b>Page</b>
2-1	State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed .....	2-2
2-2	State Legislative Activity in Health IT, 2005–2007—Legislation Introduced But Not Passed .....	2-7
2-3	State Legislative Activity in Health IT, 2005–2007—Legislation Not Introduced to Date .....	2-7
2-4	Health IT–Related Executive Orders Issued by State Governors.....	2-11



## EXECUTIVE SUMMARY

This Impact Analysis report is the seventh in a series of reports to be produced under RTI International's contract with the Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ). During the past 18 months, participating state teams<sup>1</sup> have successfully completed an assessment of the variation among business practices, policies, and laws to gain a better understanding of the privacy and security landscape within their states to prepare them to develop a comprehensive plan to protect health information that is stored and exchanged electronically. The state teams also identified practices, policies, and laws that create barriers to electronic health information exchange and have worked to develop possible solutions to these barriers that both preserve and protect privacy and security and promote interoperable electronic health information exchange. The Privacy and Security Solutions project has provided the state teams with the leadership, methodology, and funding to engage and educate stakeholders within their states and build coalitions of stakeholders across diverse areas within the health care system.

The Impact Analysis report provides an analysis of the many ways that the Privacy and Security Solutions project has impacted the landscape for electronic health information exchange both within and across the participating states. To date, the project has had the greatest impact on the following areas: legislation; executive orders; leadership and governance; stakeholder education and knowledge; and, development and sustainability of health information technology (health IT)/health information exchange efforts in the states. A separate section detailing the progress of the collaborative work groups and other cross-state initiatives and interstate projects is included.

The report consists of 6 major sections:

- Introduction
- Impact Analysis
- Collaborative (Cross-State) Outcomes
- Overview of Individual States/Territories
- Conclusions
- References

### Background

This report provides an analysis of the impact of the Privacy and Security Solutions project activities, both within and across the participating states. The primary emphasis of the

---

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

impact analysis is necessarily state-specific: state project teams have identified outcomes and impacts that are specific to their states and their unique health information exchange environments. The report also discusses impacts achieved through participation in multi- and cross-state activities. It primarily addresses the broader impacts of the project on privacy and security solutions within the states and, to a lesser degree, on larger health IT initiatives.

## **Methodology**

To assess and analyze the impacts of the Privacy and Security Solutions project and related activities, it was necessary first to examine the states' status at the start of the project. In early 2006, states and territories applying for funding to participate in Phase I of the Privacy and Security Solutions project were asked to provide an environmental scan characterizing the health IT initiatives and projects within their states and the scope of stakeholder involvement in these efforts. These environmental scan sections of the state project proposals served as the primary source of information on the states' status at the onset of the project. These findings were then compared with the states' progress in implementing solutions to address privacy and security issues in electronic health information exchange. Impacts realized during the project were identified from reviews of the states' final implementation plans, and from participation in collaborative work groups. Additional reports from state project directors were used to verify and supplement this initial information.

### ***Landscape Before the Project***

When the Privacy and Security Solutions project began, participating states were at different stages of health information exchange development. In their project proposals, all states reported some type of existing health IT and health information exchange activity. These activities included independent, isolated health IT efforts by individual health care organizations (generally done to build or expand internal IT capabilities); implementation of 1 or more local multi-organizational health information exchange efforts, which were limited in scope and participation; and early planning of a statewide electronic health information exchange. Most of these efforts were funded by the organizations themselves or with seed or start-up monies from federal, state, or private foundation sources. Only a relatively small number of states reported a high level of maturity in their local efforts, such as the establishment of foundational components of a statewide initiative, early implementation of a statewide health information exchange effort, or an operating statewide health information exchange (HIE) program. Findings from the first and second surveys of local, regional, and state health information exchange activities conducted in 2004 and 2005 by the eHealth Initiative (eHealth Initiative, 2005) and from an independent evaluation of the evolution of state HIEs (Agency for Healthcare Research and Quality, 2006) confirm this initial assessment of the status of health information exchange development across the

nation. Both studies showed that more than 100 projects related to health information exchange existed in at least 35 states. In the remaining 15 states and territories, health information exchange projects were also likely under way but not identified because of their size, scope, or early planning stage.

These studies reveal 2 important points about the early stage of health information exchange development (before the start of the Privacy and Security Solutions project):

- A relatively small number of states had a defined entity or program that was recognized as the “state HIE effort” (ie, both a defined state HIE effort and an identified independent entity or government agency that had taken the formal role of facilitating, coordinating, convening, or operating this state effort).
- No state “anchor” or multistakeholder body (whether a state committee, commission, board, or other) had been given responsibility for addressing health information privacy and security issues.

Other important factors were evident in these early stages of development:

- The underlying state infrastructure for health IT and health information exchange was lacking.
- Few states had started statewide health information exchange planning efforts, including assessments of needs and capabilities (ie, surveying state providers to assess the level of penetration of foundational health information technologies, such as electronic health records (EHRs)) or development of a framework and road map for moving forward.
- Organization and governance for a state health information exchange effort were evolving.
- The key roles of state government as a participant, convener, and coordinator were emerging.
- Ensuring consumer participation in the process was a major challenge.
- Financial models for initial development and sustainable operations were being developed.

### ***Evolution of the Landscape During the Project***

The period between 2005 and 2007 was instrumental in moving the nation closer to a transformation in health IT and health information exchange. This process has been fueled by the significant investment and national leadership that the federal government provided for these issues through the efforts of the Office of the National Coordinator for Health Information Technology, the Agency for Healthcare Research and Quality, the Centers for Medicare & Medicaid Services, the Health Resources and Services Administration, the National Library of Medicine, the Centers for Disease Control and Prevention, the Substance Abuse and Mental Health Services Administration, the Department of Veterans Affairs, the Department of Defense, and many others.

During this period state policy makers (both state governors and legislatures) and the private sector have become highly interested in health IT and health information exchange issues and have recognized their significance. Over the past 2 years alone, more than 300 state legislative initiatives related to health IT and health information exchange have been introduced across the country. A number of state governors have issued executive orders identifying, assigning, or creating state bodies to guide the development of state health information exchange efforts. Findings from the third annual survey of health information exchanges conducted by eHealth Initiative (2006), the State Level Health Information Exchange project implemented by the Foundation of Research and Education of the American Health Information Management Association (FORE/AHIMA; 2007a,b), and the National Governors Association (NGA) State Alliance for e-Health (NGA, 2007)<sup>2</sup> provide evidence of this impressive body of state policy making initiatives in support of local, regional, and state health IT and health information exchange. As documented by the National Conference of State Legislatures' (NCSL's) Health Information Technology Champions (HITCh) initiative (NCSL, 2007),<sup>3</sup> legislation adopted and enacted in 2007 alone covered 5 major areas:

- increasing state funding to support the adoption of health information technologies (such as EHRs by state providers);
- creating and supporting local and regional health information organizations and providing core funding for the implementation of a statewide HIE;
- establishing governance structures to guide and coordinate the planning and development of a statewide HIE;
- addressing privacy and security issues, such as consent approaches, and creating a state privacy and security board; and
- supporting the participation of public health and Medicaid in state HIE pilot projects and initiatives.

From 2004 (before the Privacy and Security Solutions project) to 2007, state partners made significant progress in implementing statewide health information exchange. According to reports from state project directors (supplied for the Assessment of Variation and Analysis of Solutions Report), a shift has been noted from the stages of early planning to more mature efforts establishing foundational components, early implementation, and establishing an operating statewide implementation.

---

<sup>2</sup> Information on the NGA State Alliance for e-Health is available at the website (NGA, 2007).

<sup>3</sup> NCSL's HITCh initiative is a partnership aimed at strengthening the capacity of state legislators to respond to issues related to the use of technology to improve access, quality, and effectiveness in health care. HITCh maintains a list of all introduced and enacted health IT and health information exchange state legislation. More information is available at the website (NCSL, 2007).

## Impact Analysis

The impact of the Privacy and Security Solutions project can be observed in 5 major domains: legislation, executive orders, leadership and governance, stakeholder education and knowledge, and support for health information exchanges. The information analyzed in this section was drawn from the individual state reports of progress that occurred from the beginning of the project through the conclusion of Phase II (see Section 1.2 for additional discussion of methodology). The process of the Privacy and Security Solutions project played a critical role in state teams' success. In identifying variations, developing solutions, and implementing foundational privacy and security solutions, the teams were able to build awareness of health IT and health information exchange issues across their respective states and generate momentum toward interoperability. This section addresses key areas in which states have made substantial progress as a result of the project.

### **Legislation**

States are in different stages of progress regarding legislation: some states have already passed new legislation, others have bills under active consideration, and still others are drafting legislation to be introduced in future legislative sessions in 2008 or 2009.

The Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels, conducted by the eHealth Initiative and summarized in the report *Improving the Quality of Healthcare Through Health Information Exchange* (eHealth Initiative, 2006), and a summary from the National Council of State Legislatures provides an extensive overview of legislation passed between 2005 and 2007. This includes many bills that fall under the broad umbrella of health IT. With respect to legislation, this section of the report considers a narrower set of bills, namely those where the Privacy and Security Solutions project participants directly contributed to the legislation's drafting or passage. Discussions with project directors in each of the states participating in the Privacy and Security Solutions project led to identification of additional project-related legislative activities in 11 states.

The intent of state legislation was to update and align statutes with the electronic health information environment and address legal barriers to electronic exchange. States worked diligently to mitigate the risk of codifying existing variations in business practices related to health information exchange by involving multiple stakeholders and getting feedback from a broad audience before passage. The positive impact these legislative efforts have on electronic health information exchange and how well they reduce privacy and security variations in their application among organizations who engage in electronic health information exchange will be an important measure of success.

### ***Executive Orders***

Executive orders issued by state governors are another indicator of the Privacy and Security Solutions project's impact. Some of the executive orders predate the project, and when this is the case, state teams often cited the executive order as an impetus for applying for funding under the Privacy and Security Solutions project. As a direct result of this project, executive orders have been issued in Kansas, Mississippi, and Ohio. Several states reported that executive orders are under consideration by their respective governors. The executive orders offer formal support for the project and help to sustain efforts towards interoperable exchange.

### ***Leadership and Governance***

As state teams moved through the process of identifying variations, creating solutions, and beginning implementation, many identified a need for specific privacy and security leaders to take ownership of the implementation process and oversee future steps. The Privacy and Security Solutions project was designed to support sustainable solutions for interoperable health information exchange—for example, by having state teams work closely with stakeholders and by requiring teams to secure a letter of support from their governor. The project has built on the existing leadership at the state level, allowing states to identify champions and accelerate progress toward interoperable exchange.

Before the launch of the Privacy and Security Solutions project, state-level leadership and support for health IT and health information exchange varied widely, with most states lacking well-defined, coordinated leadership. As a result of the Privacy and Security Solutions project, state teams generally reported the formation of 3 types of leadership structures: government-supported boards, commissions, or task forces (15 states); leadership structures of HIE entities (3 states); and convenor organizations (4 states). The leadership of HIEs and convenor organizations has continued, and state teams have built from the existing expertise and commitment, even though the work of the government-supported initiatives was often limited by time or task objectives.

The Privacy and Security Solutions project has also proved significant in its reach. Many state teams reported much higher levels of interest from governors, legislators, and state agencies than existed before the project. This reported increase in interest is supported by the increased number of introduced bills and executive orders related to health IT and health information exchange that occurred during the contract span. State teams also received support in other ways, such as the endorsement of the Privacy and Security Solutions state project teams and the establishment of steering committees by their legislative and executive branches.

### ***Stakeholder Education and Knowledge***

A key goal of the Privacy and Security Solutions project was for state teams to create a broad base of support among stakeholders in their states to develop consensus solutions and sustainability that would extend beyond the contract period. The Privacy and Security Solutions project provided state teams with the resources to engage a broader range of stakeholders than would have been possible otherwise. Similarly, it afforded states the resources to engage on a broader array of issues.

One of the key developments in this area is the understanding that privacy and security are essential components of exchange. Similarly, state teams have also realized that the technology to support exchange exists, and that policies, workflow considerations, and broad stakeholder buy-in must be established for successful exchange. Using the resources and tools provided through participation in the project, state project teams were able to examine the business practices for the exchange of health information not only in direct patient care, but also within a broader context. The 18 specific scenarios that were developed and used in the examination of business practices covered the following areas: treatment; payment; regional health information organizations (RHIOs); research data use; law enforcement; prescription drug use/benefit; health care operations/marketing; bioterrorism; employee health; public health; and state government oversight. A broad representation of stakeholder groups ensured that the project's review of variations and legal drivers would be comprehensive, and that a coalition of support would form and be sustained within the states to ensure that solutions developed and implementation plans would be carried forward successfully.

### ***Development and Sustainability of Health IT/HIE Efforts in the States***

The Privacy and Security Solutions project has helped states establish a privacy and security foundation with which to develop new health IT efforts. Moreover, state teams have reported increased engagement of stakeholders in the development and continuation of health IT efforts. As the state teams develop privacy and security solutions and implement them, they decrease barriers for other health IT and health information exchange efforts. This work is supported by the progress of existing projects to higher levels of development, and has fostered the development of new HIEs.

### ***Collaborative (Cross-State) Outcomes***

Almost unanimously, states reported that working with 33 other states and territories on the Privacy and Security Solutions project proved extremely valuable in understanding their state-specific challenges for health IT and health information exchange within a larger nationwide framework.

The relationships that the states have forged, or are planning to pursue, reflect a variety of cross-state interests. A number of states have established better communications with

states in their geographical area. Many states, however, have developed relationships that are based on shared interests, not on geographical proximity. Some states need to share health information with distant states because their citizens often travel between them for vacations or health care. Other states have formed relationships to share information about common approaches to health information exchange architecture, issues, or projects.

### ***Collaborative Work Groups***

To increase the focus on cross-state collaboration, RTI was tasked with coordinating and overseeing the formulation of multistate, collaborative work groups during the extension period (June through December 2007) of the Privacy and Security Solutions project. Seven collaborative work groups have been focused on the following areas:

- consumer education and engagement
- provider education
- standards policy adoption
- harmonizing state privacy law
- consent options, outcomes, and best practices
- consent data elements required for data transfer
- interorganizational agreements

### ***Other Cross-State Initiatives and Interstate Projects***

In addition to the formal multistate collaborative groups formed under the Privacy and Security Solutions project, a number of states have reported laying foundations for or undertaking cross-state projects as part of the Privacy and Security Solutions project work. Some of these cross-state interactions resulted from networking opportunities provided by the project. Many states were able to point to distinct instances in which discussions with other states served as a significant resource informing their own projects. The potential for multistate and cross-collaborative work between the states is exceptionally strong, especially given the foundation that has been provided by the Privacy and Security Solutions project.

### **Overview of Individual States/Territories**

Section 4 in this report summarizes the impact of the Privacy and Security Solutions project on the individual states participating in the project. Participating states are presented in alphabetical order. Each state's report includes 3 sections. The first section, Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project, describes the status of electronic health information exchange that existed before the project began. These descriptions have been drawn primarily from the proposals submitted by each state to be part of the project. The intent of this section is to provide the context for

understanding the impact of the project and describe the particular challenges faced in each state related to factors such as geography, population, and the health care delivery system. The second section, Current Health IT/HIE Landscape, captures changes that have occurred since those proposals were submitted, drawn from project reports on activities in each state, review of websites and other available material, and verified in discussions with key project staff in each state. The section describes progress made toward exchanging health information, such as the development of RHIOs or similar entities, or efforts to expand the exchange of health information. The third section for each state, Current Privacy and Security Landscape, focuses on privacy and security impacts within each state and also draws primarily from project reports and discussions with key project staff. This section is intended to provide detail about the heightened awareness of privacy and security issues in each state and the actions state teams have taken as a result of their participation in the Privacy and Security Solutions project.

## **Conclusions**

This report provides a comprehensive review of the work conducted under the Privacy and Security Solutions project. It is clear that the 34 state teams have made substantial progress toward the reaching the goals stated at the outset of the project, which include:

- Assess variations in organization-level business policies and state laws that affect health information exchange;
- Identify and propose practical solutions, while preserving the privacy and security requirements in applicable federal and state laws, and;
- Develop detailed plans to implement solutions.

This report describes the progress that state teams have made during the past 18 months toward meeting these goals. The teams have identified the sources of variation that must be reduced to arrive at a common set of policies that will permit private and secure nationwide health information exchange. They have worked to educate and engage the stakeholders within their individual states, laying the groundwork for an enduring statewide constituency through which they can work to achieve consensus on the implementation of solutions. The state teams now have an infrastructure in place that positions them to work toward harmonizing privacy practices, policies, and laws both within their individual states and across states. They are also leaving behind in states and communities a knowledge base about privacy and security issues in electronic health information exchange that endures to inform future health information exchange activities. The next steps for the state teams include accelerating the implementation of solutions by working in multistate collaboratives, developing dissemination pathways to achieve widespread adoption, and coordinating with the other national initiatives.



# 1. INTRODUCTION

## 1.1 Background

This Impact Analysis Report is the seventh in a series of reports to be produced under RTI International's contract with the Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ). During the past 18 months, participating state teams<sup>4</sup> have successfully completed an assessment of the variation among business practices, policies, and laws to gain a better understanding of the privacy and security landscape within their states to prepare them to develop a comprehensive plan to protect health information that is stored and exchanged electronically. The state teams also identified practices, policies, and laws that create barriers to electronic health information exchange and have worked to develop possible solutions to these barriers that both preserve and protect privacy and security and promote interoperable electronic health information exchange. The Privacy and Security Solutions project has provided the state teams with the leadership, methodology, and funding to engage and educate stakeholders within their states and build coalitions of stakeholders across diverse areas within the health care system.

This report provides an analysis of the impact of the Privacy and Security Solutions project activities, both within and across the participating states. The primary emphasis of the impact analysis is necessarily state-specific: state project teams have identified outcomes and impacts that are specific to their states and their unique health information exchange environments. The report also discusses impacts achieved through participation in multi- and cross-state activities. It primarily addresses the broader impacts of the project on privacy and security solutions within the states and, to a lesser degree, on larger health information technology (health IT) initiatives.

State teams have found a wide range of project impacts within their states. Both the nature and the extent of these impacts are related to the states' prior levels of health IT development. Some states that were further along in their health IT implementations were able to develop and adopt privacy and security policies that were then adopted by the HIEs and regional health information organizations in their states. Others, just beginning discussions related to interoperable health information exchange, were able to bring a diverse group of stakeholders together and begin to address the identified barriers. Several states were able to enact legislation necessary to update their state statutes from a paper-based environment to one conducive to interoperable health information exchange in the electronic environment.

---

<sup>4</sup> Throughout this report the 33 states and 1 territory are referred to as the state project teams or as the state teams.

Section 2 of this report addresses 5 specific areas of impact: legislation, executive orders, leadership and governance, stakeholder education and knowledge, and development and sustainability of health IT and health information exchange efforts in the states. Section 3 discusses cross-state initiatives and multistate collaborative work groups, along with their resulting impacts. Section 4 provides individual state summaries, focusing on impacts that have been realized since the Privacy and Security Solutions project began. Finally, Section 5 summarizes results and provides conclusions.

## **1.2 Methodology**

To assess and analyze the impacts of the Privacy and Security Solutions project and related activities, it was necessary first to examine the states' status at the start of the project. In early 2006, states and territories applying for funding to participate in Phase I of the Privacy and Security Solutions project were asked to provide an environmental scan characterizing the health IT initiatives and projects within their states and the scope of stakeholder involvement in these efforts. These environmental scan sections of the state project proposals served as the primary source of information on the states' status at the onset of the project. These findings were then compared with the states' progress in implementing solutions to address privacy and security in electronic health information exchange. Impacts realized during the project were identified from reviews of the states' final implementation plans, and from participation in collaborative work groups. Additional reports from state project directors were used to verify and supplement this initial information.

## **1.3 The Privacy and Security Solutions Project and the Evolving State and Nationwide Landscape of Health IT and Health Information Exchange**

### ***1.3.1 Landscape Before the Project***

When the Privacy and Security Solutions project began, participating states were at different stages of health information exchange development. In their project proposals, all states reported some type of existing health IT and health information exchange activity. These activities included independent, isolated health IT efforts by individual health care organizations (generally done to build or expand internal IT capabilities); implementation of 1 or more local multi-organizational health information exchange efforts, which were limited in scope and participation; and early planning of a statewide electronic health information exchange. Most of these efforts were funded by the organizations themselves or with seed or start-up monies from federal, state, or private foundation sources. Only a relatively small number of states reported a high level of maturity in their local efforts, such as the establishment of foundational components of a statewide initiative, early implementation of a statewide health information exchange effort, or an operating statewide HIE program. Findings from the first and second surveys of local, regional, and state health information exchange activities conducted in 2004 and 2005 by the eHealth Initiative (eHealth Initiative,

2005) and from an independent evaluation of the evolution of state HIEs (Agency for Healthcare Research and Quality, 2006) confirm this initial assessment of the status of health information exchange development across the nation. Both studies showed that more than 100 projects related to health information exchange existed in at least 35 states. In the remaining 15 states and territories, health information exchange projects were also likely under way but not identified because of their size, scope, or early planning stage.

These studies reveal 2 important points about the early stage of health information exchange development (before the start of the Privacy and Security Solutions project):

- A relatively small number of states had a defined entity or program that was recognized as the “state HIE effort” (ie, both a defined state HIE effort and an identified independent entity or government agency that had taken the formal role of facilitating, coordinating, convening, or operating this state effort).
- No state “anchor” or multistakeholder body (whether a state committee, commission, board, or other) had been given responsibility for addressing health information privacy and security issues.

Other important factors were evident in these early stages of development:

- The underlying state infrastructure for health IT and health information exchange was lacking.
- Few states had started statewide health information exchange planning efforts, including assessments of needs and capabilities (ie, surveying state providers to assess the level of penetration of foundational health information technologies, such as electronic health records (EHRs)) or development of a framework and road map for moving forward.
- Organization and governance for a state health information exchange effort were evolving.
- The key roles of state government as a participant, convener, and coordinator were emerging.
- Ensuring consumer participation in the process was a major challenge.
- Financial models for initial development and sustainable operations were being developed.

### ***1.3.2 Evolution of the Landscape During the Project***

The period between 2005 and 2007 was instrumental in moving the nation closer to a transformation in health IT and health information exchange. This process has been fueled by the significant investment and national leadership that the federal government provided for these issues through the efforts of the Office of the National Coordinator for Health Information Technology, the Agency for Healthcare Research and Quality, the Centers for Medicare & Medicaid Services, the Health Resources and Services Administration, the National Library of Medicine, the Centers for Disease Control and Prevention, the Substance

Abuse and Mental Health Services Administration, the Department of Veterans Affairs, the Department of Defense, and many others.

During this period state policy makers (both state governors and legislatures) and the private sector have become highly interested in health IT and health information exchange issues and have recognized their significance. Over the past 2 years alone, more than 300 state legislative initiatives related to health IT and health information exchange have been introduced across the country. A number of state governors have issued executive orders identifying, assigning, or creating state bodies to guide the development of state health information exchange efforts. Findings from the third annual survey of health information exchanges conducted by eHealth Initiative (2006), the State Level Health Information Exchange project implemented by the Foundation of Research and Education of the American Health Information Management Association (FORE/AHIMA; 2007a,b), and the National Governors Association (NGA) State Alliance for e-Health (NGA, 2007)<sup>5</sup> provide evidence to this impressive body of state policymaking initiatives in support of local, regional, and state health IT and health information exchange. As documented by the National Conference of State Legislatures' (NCSL's) Health Information Technology Champions (HITCh) initiative (NCSL, 2007),<sup>6</sup> legislation adopted and enacted in 2007 alone covered 5 major areas:

- increasing state funding to support the adoption of health information technologies (such as EHRs by state providers);
- creating and supporting local and regional health information organizations and providing core funding for the implementation of a statewide HIE;
- establishing governance structures to guide and coordinate the planning and development of a statewide HIE;
- addressing privacy and security issues, such as consent approaches, and creating a state privacy and security board; and
- supporting the participation of public health and Medicaid in state HIE pilot projects and initiatives.

From 2004 (before the Privacy and Security Solutions project) to 2007, state partners made significant progress in implementing statewide health information exchange. According to reports from state project directors (supplied for the Assessment of Variation and Analysis of Solutions Report), a shift has been noted from the stages of early planning to more mature efforts establishing foundational components, early implementation, and establishing an operating statewide implementation.

---

<sup>5</sup> Information on the NGA State Alliance for e-Health is available at the website (NGA, 2007).

<sup>6</sup> NCSL's HITCh initiative is a partnership aimed at strengthening the capacity of state legislators to respond to issues related to the use of technology to improve access, quality, and effectiveness in health care. HITCh maintains a list of all introduced and enacted health IT and health information exchange state legislation. More information is available at the website (NCSL, 2007).

## 2. IMPACT ANALYSIS

Section 2 describes the impact of the Privacy and Security Solutions project in 5 major domains: legislation, executive orders, leadership and governance, stakeholder education and knowledge, and support for health information exchanges (HIEs). The initiatives resulting from this project have brought about changes in business practices, policies, and state law; educational efforts aimed at providers and consumers; and several other approaches to reduce privacy and security variations related to the exchange of health information.

The analysis in this section was drawn from the individual state reports of progress that occurred from the beginning of the project through the conclusion of Phase II (see Section 1.2 for additional discussion of methodology). The process of the Privacy and Security Solutions project played a critical role in state teams' success. In identifying variations, developing solutions, and implementing foundational privacy and security solutions, the teams were able to build awareness of health information technology (health IT) and health information exchange issues across their respective states and generate momentum toward interoperability. As a result of the project, states have made substantial progress in the following key areas.

### 2.1 Legislation

States are in different stages when it comes to legislation: some states have already passed new legislation, others have bills under active consideration, and still others are drafting legislation to be introduced in future legislative sessions in 2008 or 2009. In many states these activities preceded the project implementation and served, in part, to motivate participation in the project. In other states, such as Michigan and Minnesota, the work of the state project teams contributed to legislation enacted during the project. In addition, a number of states, including Rhode Island and New Hampshire, plan to introduce legislation in the upcoming session.

The Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels, conducted by the eHealth Initiative and summarized in the report *Improving the Quality of Healthcare Through Health Information Exchange* (eHealth Initiative, 2006), and a summary from the National Council of State Legislatures (NCSL) provides an extensive overview of legislation passed between 2005 and 2007. The eHealth Initiative survey was fielded in May 2006, partway through the Privacy and Security Solutions project schedule. Survey respondents included health information exchange initiatives in 49 states, the District of Columbia, and Puerto Rico. The report documents 121 health IT-related bills introduced in 38 states since 2005, with 36 bills passed and signed into law in 24 states (eHealth Initiative, 2006, pp. 9–10). The NCSL Health Information Technology Champions group states that by 2007 more than 250 health IT-related bills

were introduced, with 59 passed in 34 states, plus the District of Columbia. Tables 2-1 through 2-3 summarize this activity. The information contained in these tables is current as of December 14, 2007, and is based on the sources listed. There may be some pieces of legislation missing based on when the eHealth Initiative and NCSL conducted their surveys.

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed**

---

Alabama
<b>Act 2007-171, AL HJR 176</b> – Enacted 04/16/2007 - Establishes the Health Information Technology Partnership.
Arizona <sup>a</sup>
<b>Chapter 255, AZ H 2781</b> – Enacted 06/25/2007 - Appropriates funds for electronic medical records.
Arkansas <sup>a</sup>
<b>Act 1283, AR H 1354</b> – Enacted 04/05/2007 - Includes funding for the Health Department Technology Fund and for Information Technology Initiative activities of the Department of Health.
California <sup>a</sup>
<b>CA SB 1039</b> – Enacted 10/11/2007 - Makes technical and conforming changes to the Public Health Act of 2006. Establishes new functions and responsibilities for the State Department of Public Health and the State Department of Health Care Services.
Connecticut <sup>a</sup>
<b>House Bill No. 8002</b> – Enacted 06/26/2007 – Implements the provisions of the budget concerning human services and public health.
<b>Senate Bill No. 1484</b> – Enacted 07/10/2007 – Concerns the HealthFirst Connecticut and Healthy Kids initiatives.
Colorado <sup>a</sup>
<b>Chapter 282, CO S 196</b> – Enacted 05/24/2007 - Creates the health IT advisory committee to develop a long-range plan for health care information technology.
<b>Chapter 319, CO H 1346</b> – Enacted 05/29/2007 - Allows for increased fees to cover use and maintenance of electronic health records to contractors within the Medical Assistance Program.
<b>Chapter 296, CO S 74</b> – Enacted 05/25/2007 - Creates the emergency access to health information demonstration program.
Delaware
<b>DE S 155</b> – Enacted 07/01/2007 - Appropriates funds for the Delaware Health Information Network.
District of Columbia
<b>DC B 2</b> – Enacted 01/16/2007 - Includes appropriations for electronic health records system in community health centers.

---

(continued)

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed (continued)**

<p>Florida<sup>a</sup></p> <p><b>House Bill No. 7073</b> – Enacted 06/20/2006 - Renaming the State Center for Health Statistics; revising criteria for collection and use of certain health-related data; providing responsibilities of the Agency for Health Care Administration; providing for agency consultation with the State Consumer Health Information and Policy Advisory Council for the dissemination of certain consumer information; requiring the Florida Center for Health Information and Policy Analysis to provide certain technical assistance services...</p> <p><b>Senate Bill No. 1408</b> – Enacted 07/01/2006 – An act relating to medical records; amending s. 456.057, F.S.; providing definitions; requiring a health care practitioner's employer who is a records owner and a records custodian to comply with specified requirements for confidentiality and disclosure; amending s. 456.42, F.S.; providing requirements for prescriptions of medicinal drugs by health care practitioners which are electronically generated or transmitted; creating s. 456.43, F.S.; regulating electronic prescribing for medicinal drugs; providing restrictions for electronic prescribing software; providing definitions; authorizing electronic prescribing software to show information regarding a payor's formulary under certain circumstances; ...</p>
<p>Georgia</p> <p><b>GA H 94</b> – Enacted 04/19/2007 – Provides funding to the Georgia Association for Primary Health Care to complete the statewide electronic medical records system to link the Federally Qualified Community Health Centers.</p>
<p>Idaho</p> <p><b>ID H 159</b> – Enacted 03/27/2007 – Creates a Community Health Center Grant Fund with the intent of improving access to health care services through grants.</p>
<p>Illinois<sup>a</sup></p> <p><b>IL S 3866</b> – Enacted 08/23/2007 – Funds expenses of the Adoption Registry and Medical Information Exchange.</p>
<p>Indiana<sup>a</sup></p> <p><b>Public Law 111, IN S 551</b> – Enacted 05/02/2007 – Establishes the Health Informatics Corporation.</p>
<p>Iowa<sup>a</sup></p> <p><b>IA H 451</b> – Enacted 04/20/2007 - Creates a single point of entry long-term living resource systems team. The team will issue a report to the general assembly by December 1, 2008, that includes recommendations regarding the use of electronic health records.</p> <p><b>IA H 909</b> – Enacted 05/29/2007 - Makes appropriations procurement and installation for electronic medical records within a state facility.</p>
<p>Kansas<sup>a</sup></p> <p><b>KS H 2368</b> – Enacted 04/23/2007 - Appropriates funds to support ongoing health information exchange initiatives that include health information exchange infrastructure planning, privacy and security collaboration, the advanced identification card project and the community health record project and to support the inclusion of disease management, a strengthening of electronic prescribing and electronic medical records, and the development of pilot programs and compatibility with the private sector.</p>

(continued)

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed (continued)**

---

Kentucky<sup>a</sup>

**SB 2** – Enacted 03/08/2005 – Calls for the development and implementation of a statewide Kentucky e-Health Network, or Ke-HN. The goal of Ke-HN is to improve the quality and reduce the cost of health care for Kentuckians.

---

Louisiana<sup>a</sup>

**Act 243, LA S 1** – Enacted 07/06/2007 – Authorizes the Department of Health and Hospitals to develop and implement a health care delivery system for Medicaid recipients and low-income uninsured citizens.

**Act 172, LA S 238** – Enacted 06/27/2007 – Establishes the Health Care Redesign Fund in the state treasury.

**Act 203, H 765** – Enacted 06/27/2007 – Payable out of the State General Fund (Direct) for implementation of Phase I of the statewide electronic medical records system for state public hospitals and medical centers.

---

Maine<sup>a</sup>

**Chapter 72, ME H 548** – Enacted 05/04/2007 –Expands the definition of health care facility under the Maine Health and Higher Educational Facilities Authority Act.

---

Maryland

**MD H 979** – Enacted 04/24/2007 – Establishes a health information exchange pilot project.

---

Massachusetts<sup>a</sup>

**MA H 4141**– Enacted 07/12/2007 – Appropriates funds for fiscal year 2008.

**MA H 4160** – Enacted 10/10/2007 – Establishes an electronic health records task force.

---

Michigan<sup>a</sup>

**Public Act 7, MI S 404** – Enacted 05/07/2007 – Appropriations for the Medical Services Administration for health IT initiatives.

**MI S1** – Enacted 10/01/2007 – Requests a federal waiver for incentives for Medicaid recipients.

---

Minnesota<sup>a</sup>

**Chapter 147, MN H 1078** – Enacted 05/25/2007 – To develop a statewide plan, including uniform standards to be used for meeting the 2015 goal, of providing an interoperable system for sharing and synchronizing patient data across systems.

**Chapter 148, MN H 548** – Enacted 05/25/2007 – To establish an enterprise-wide pilot project to provide consumer-owned electronic personal health records to employees of Minnesota state colleges and universities and all participants in the state employee group insurance program.

**Chapter 144, MN H 1063** – Enacted 05/30/2007 – Appropriates funds for higher education if certain conditions are met for increased training of students on the use of electronic medical record technology.

---

Missouri

**MO S 577** – Enacted 07/02/2007 – Among other things creates a Healthcare Technology Fund.

**MO H 11** – Enacted 06/27/2007 – Funds an electronic pilot project in 1 or more skilled nursing facilities in Greene County to study the cost effectiveness of electronic health records in long-term care and the financial benefit to Missouri HealthNet from the Nursing Facility Quality of Care Fund.

---

(continued)

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed (continued)**

Montana
<b>MT D 683, MT SJR 19</b> – Enacted 04/24/2007 – Relates to developing health IT.
Nebraska
<b>LB 185 Section 71-5185</b> – 2007 – Language was changed to allow the 2-way exchange of electronic medical information and to clarify rights and protections.
Nevada
<b>Chapter 423, NV S 536</b> – Enacted 06/13/2007 – HIPPA-covered entities that transit individually identifiable health information in compliance with HIPPA provisions are exempt from more stringent state laws. The bill also allows individuals to opt out of electronic transmission of individually identifiable health information with an exceptions for Medicaid and SCHIP patients and when required by HIPPA or state law.
New Hampshire <sup>a</sup>
<b>HB 514</b> – Enacted 05/26/2005 –Establishes the New Hampshire health care quality assurance commission to enable health care providers to share information about adverse outcomes and prevention strategies in learning environments which foster candor and self-critical analysis while maintaining the confidentiality of the information submitted to the commission, the proceedings of the commission, and the results of the commission’s deliberations.
New Mexico
<b>Chapter 007-21, NM S 611</b> – Enacted 03/13/2007 – To purchase electronic health records software for the Mora Valley community health center.
<b>NM HM 60</b> – Enacted 03/07/ 2007 – Asks the health and human services committee to conduct a board review of health care reform including health IT.
New York <sup>a</sup>
<b>Chapter 54, NY S 2104</b> – Enacted 04/09/2007 – For services and expenses of health IT.
North Dakota
<b>ND H 1021</b> – Enacted 05/02/2007 - Appropriates funds for the Information Technology Department and creates a health IT steering committee.
Ohio <sup>a</sup>
<b>OH H 119</b> – Enacted 06/30/2007 - Establishes the health information and imaging technology workforce development pilot project.
Oklahoma <sup>a</sup>
<b>OK H 1818</b> – Engrossed 02/14/2007 – Creates a task force on health care IT.
Oregon
<b>OR S 329</b> – Enacted 06/28/2007 – Develops recommendations for a model quality institute that provides leadership and support to further the development of widespread and shared electronic health records; and develops the capacity of the workforce to capitalize on health IT.

(continued)

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed (continued)**

---

Rhode Island <sup>a</sup>
<b>H 7120</b> – Enacted 06/24/2006 – A new state budget under which the state agreed to contribute \$6 million to help finance the cost of building a regional health information organization, subject to certain conditions.
Tennessee
<b>SB 2268</b> – Enacted 06/06/2007 - Requires approval from the Commissioner of Finance and Administration for all state contracts for the development or purchase of health IT with other states and federal agencies.
Texas
<b>TX H 1066</b> – Enacted 06/15/2007 – Relates to electronic health information and electronic health records; creates the Texas Health Service Authority Corporation.
<b>TX S 10</b> – Enacted 06/14/2007 – Creating health care systems efficiencies, such as using electronic medical records systems.
<b>TX H 522</b> – Enacted 05/25/2007 – Establishes an advisory committee on health information exchange; establishes an identification card pilot project program.
<b>TX S 11</b> – Enacted 06/06/2007 – Relating to homeland security and protection of the public, including protections against human trafficking; providing penalties.
Vermont <sup>a</sup>
<b>Act 27, VT H 380</b> – Enacted 05/16/2007 – Amends hospital reporting and licensing requirements...
<b>Act 70, VT H 229</b> – Enacted 06/05/2007 – Makes corrections and clarifications to the 2006 Health Care Affordability Act and related legislation.
<b>Act 71, VT H 531</b> – Enacted 06/04/2007 – Establishes outreach and enrollment principles for Catamount Health and state benefit programs; establishes the rural health alliance. Requires that all primary care providers participating in the project use health IT.
Virginia
<b>Chapter 847, VA H 1650</b> – Enacted 04/04/2007 – Appropriates public revenues.
<b>Chapter 635, VA H 2198</b> – Enacted 03/20/2007 –Requires any electronic health records system or software purchased by a state agency to adhere to accepted standards for interoperability or to be certified by a recognized certification body.
Washington <sup>a</sup>
<b>Chapter 259, WA S 5930</b> – Enacted 05/02/2007 – Provides high quality, affordable health care to residents based on the recommendations of the blue ribbon commission on health care costs and access.
<b>Chapter 2007-522, WA H 1128</b> – Enacted 05/15/2007 – Makes appropriations for 2007–2009.
<b>Chapter 114, WA S 5640</b> – Enacted 04/18/2007 – Through state health purchasing, reimbursement, or pilot strategies, promotes and increases the adoption of health IT systems, including electronic medical records.

---

(continued)

**Table 2-1. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced and Passed (continued)**


---

West Virginia <sup>a</sup>
<b>Senate Bill No. 170</b> – Enacted 06/09/2006 – Relating to the establishment of the West Virginia Health Information Network; establishing purpose of the network; setting up a board of directors; establishing membership and terms of office of the board; permitting promulgation of legislative rules; establishing the powers and duties of the network; setting up a special revenue account; immunity from liability; property rights; dispute resolution; and confidentiality and privacy of records.

---

<sup>a</sup> Participant in the Privacy and Security Solutions project.

Source: Adapted from *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels*, eHealth Initiative, 2006; and from *2007 Enacted Legislation on Health Information Technology*, NCSL website, 2007.

**Table 2-2. State Legislative Activity in Health IT, 2005–2007—Legislation Introduced But Not Passed**


---

Alaska <sup>a</sup>
Hawaii
New Jersey
North Carolina <sup>a</sup>
Pennsylvania
Wisconsin <sup>a</sup>
Wyoming <sup>a</sup>

---

<sup>a</sup> Participant in the Privacy and Security Solutions project.

Source: Adapted from *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels*, eHealth Initiative, 2006; and from *2007 Enacted Legislation on Health Information Technology*, NCSL website, 2007.

**Table 2-3. State Legislative Activity in Health IT, 2005–2007—Legislation Not Introduced to Date**


---

Mississippi <sup>a</sup>
South Dakota

---

<sup>a</sup> Participant in the Privacy and Security Solutions project.

Source: Adapted from *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels*, eHealth Initiative, 2006; and from *2007 Enacted Legislation on Health Information Technology*, NCSL website, 2007.

Discussions with project directors in each of the states participating in the Privacy and Security Solutions project led to the identification of additional project-related legislative activities in 11 states (Arizona, Kentucky, Louisiana, Michigan, Minnesota, New Hampshire, New Jersey, New Mexico, Rhode Island, Vermont, and West Virginia) discussed in more detail below. Nebraska, which used tools generated by the project but did not participate directly, also identified legislation related to their review. The reported legislative activities fall into 3 categories: bills that have been enacted, bills that have been filed and are at various stages of review, and proposals that will be introduced in future legislative sessions, either in 2008 or 2009.

The project director of the Louisiana team identified recently passed legislation stemming from that team's implementation report. Louisiana SCR 75 and HCR 35 create the Louisiana Health Care Quality Foundation, which will address health IT, among other topics. The team in Michigan also identified recently passed legislation, including privacy and security measures in health IT. The Michigan team is also in the process of making legislative recommendations to the Health Information Technology Commission, which would then make recommendations to the Department of Community Health, which would then introduce legislation. The team in Minnesota noted that its work led to updates to privacy and security legislation in the state. Minnesota HF 1078 modifies existing statute in several ways, including requiring the Commissioner of Health to develop a form to enable patients to access their health records. Additional components of the legislation clarify definitions of several terms and specify terms for the exchange of health information between providers. The West Virginia teams referred to 2 bills passed in the most recent session that were a result of that team's efforts on this project. These include West Virginia HB 3184, a bill to amend an existing state statute by providing greater flexibility regarding the disclosure of confidential mental health information, and West Virginia SB 1001, a bill to amend an existing state statute by adding a new section relating generally to the authorization of electronic prescribing. Although Nebraska did not participate in the Privacy and Security Solutions project, legislation related to the storage and transmission of electronic health records was passed in Nebraska in February 2007, and the executive branch is considering additional legislation.

In New Hampshire, potential revisions to New Hampshire Statute Chapter 332-I would clarify language about ownership of medical records, specify penalties for misuse of data, and call for the creation of a uniform consent form and a commission to develop consent-form language. Legislation to amend 332-I has been filed and will be taken up for consideration by the New Hampshire legislature in 2008. The legislation has bipartisan support among state legislators, and support from the governor. Legislation in New Jersey now refers specifically to the Privacy and Security Solutions project work as the foundation for revisions to state law. New Jersey bill A 4044, "The New Jersey Health Information Technology Promotion Act," passed the Assembly by a 73-0 margin, and an identical bill,

S 2728, is currently under consideration by the Senate. Members of the New Jersey team have been working closely with state legislators to craft additional amendments to the Senate bill that would move the state beyond study of health IT issues and into implementation. The team noted that if they fail to pass the Senate bill in the current session, they plan to reintroduce it in the subsequent session.

Specific contributions to legislation in process were noted by Arizona, New Mexico, Rhode Island, and Vermont. Kentucky noted contributions to possible regulatory changes. Arizona's statutory and regulatory amendment proposals will address barriers identified in the first phase of the Privacy and Security Solutions project, specifically those related to communicable disease, mental health, immunization, and genetic testing information, and processes for subpoenas for medical records, as defined in the state's final implementation plan. Further, Arizona's Legal Work Group will continue to work on creating a new statute governing enforcement/penalties for inappropriate access to an HIE and immunity for providers and other authorized individuals who access information in an HIE in an appropriate fashion. The New Mexico proposal would address several topics, including electronic signatures, disclosure of health information, privacy protections for patients, and penalties for inappropriate disclosures. Both Arizona and New Mexico are still in the early stages of drafting legislation and plan to have materials ready for the 2009 legislative sessions.

Rhode Island's draft legislation pertains to the protection of information within the state's planned HIE. Language has been drafted and approved by the Rhode Island Quality Institute's (RIQI) board. The draft legislation has been referred to RIQI's public affairs office, which will develop a legislative strategy. Rhode Island plans to introduce a bill in its next legislative session. Vermont is exploring the possibility of updating statutes related to emergency access of health data, and is also considering expanding the role of the state ombudsman to include privacy and security of health information exchange within the state. Finally, the Kentucky team is contemplating putting forth regulatory changes that would implement a model licensing transfer agreement for use across the state.

The intent of state legislation was to update and align statutes with the electronic health information environment and address legal barriers to electronic exchange. States worked diligently to mitigate the risk of codifying existing variations in business practices related to health information exchange by involving multiple stakeholders and getting feedback from a broad audience before passage. The positive impact these legislative efforts have on electronic health information exchange and how well they reduce privacy and security variations in their application, among organizations who engage in electronic health information exchange, will be an important measure of success.

In addition to the work directly attributable to the Privacy and Security Solutions project, broader health IT legislation has been on many states' agendas. The National Conference of

State Legislatures notes that as of October 25, 2007, 53 health IT–related bills had been enacted in 32 states and the District of Columbia.<sup>7</sup>

## **2.2 Executive Orders**

Executive orders issued by state governors are another indicator of the Privacy and Security Solutions project’s impact. Some of the executive orders predate the project, and when this is the case, state teams often cited the executive order as an impetus for applying for funding under the Privacy and Security Solutions project. As a direct result of this project, executive orders have been issued in Kansas, Mississippi, and Ohio. Several states reported that executive orders are under consideration by their respective governors. The executive orders offer formal support for the project and help to sustain efforts towards interoperable exchange.

The eHealth Initiative report (2006) documents executive orders issued by governors in 10 states (Table 2-4).

On February 8, 2007, the governor of Kansas issued an executive order creating a health information exchange commission consisting of most of the project members in the state. Mississippi’s governor also issued an executive order in 2007 creating the Health Information Infrastructure Task Force. The task force is responsible for developing recommendations for the adoption and enhancement of health IT and health information exchange, including recommendations to address privacy and security issues in the adoption of health IT and to ensure privacy and security of health information exchange. In Oklahoma, the governor plans to issue an executive order to make the Privacy and Security Solutions steering committee a permanent standing body to advise on privacy and security issues related to health IT implementation. Finally, the Wyoming team noted that the governor may issue an executive order based on the team’s recommendations.

## **2.3 Leadership and Governance**

As state teams moved through the process of identifying variations, creating solutions, and beginning implementation, many identified a need for specific privacy and security leaders to take ownership of the implementation process and oversee future steps. The Privacy and Security Solutions project was designed to support sustainable solutions for interoperable health information exchange—for example, by having state teams work closely with stakeholders and by requiring teams to secure a letter of support from their governor. The project has built on the existing leadership at the state level, allowing states to identify champions and accelerate progress toward interoperable exchange.

---

<sup>7</sup> Reference: <http://www.ncsl.org/programs/health/forum/Hitch/enacted.htm>

**Table 2-4. Health IT–Related Executive Orders Issued by State Governors**

State	Date Issued	Governor
Arizona <sup>a</sup>		
Executive Order 2005 - 25	August 30, 2005	Napolitano
California <sup>a</sup>		
Executive Order S-12-06	July 24, 2006	Schwarzenegger
Florida <sup>a</sup>		
Executive Order 04-93	May 4, 2004	Bush
Illinois <sup>a</sup>		
Executive Order 9	July 13, 2006	Blagojevich
Kansas <sup>a</sup>		
Executive Order 04-14	December 14, 2004	Sebelius
Executive Order 07-02	February 8, 2007	
Mississippi <sup>a</sup>		
Executive Order 979	March 2007	Barbour
Missouri <sup>a</sup>		
Executive Order 06-03	January 17, 2006	Blunt
Ohio <sup>a</sup>		
Executive Order 2007 – 30S	September 17, 2007	Strickland
Tennessee <sup>a</sup>		
Executive Order 35	April 6, 2006	Bredesen
Virginia		
Executive Order 30	July 20, 2006	Kaine
Wisconsin <sup>a</sup>		
Executive Order 129	November 2, 2005	Doyle

<sup>a</sup> Participant in the Privacy and Security Solutions project.

Source: Adapted from *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels*, eHealth Initiative, 2006; and from *2007 Enacted Legislation on Health Information Technology*, NCSL website, 2007.

Before the launch of the Privacy and Security Solutions project, state-level leadership and support for health IT and health information exchange varied widely. State teams generally reported 3 types of existing leadership: government-supported boards, commissions, or task forces (15 states); leadership structures of HIE entities (3 states); and convenor organizations (4 states). In addition, New York and Florida were in the process of awarding grants to support health information exchange, under the Health Care Efficiency and Affordability Law for New Yorkers and Florida Health Information Network programs, respectively. The leadership of HIEs and convenor organizations has continued, and state teams have built from the existing expertise and commitment, even though the work of the government-supported initiatives was often limited by time or task objectives.

During the project, state teams recognized a need for increased leadership to serve as a resource for stakeholders within the state and to support advancement. When drafting their

implementation plans, most teams recommended that an oversight body be implemented to govern privacy and security issues across the state. These recommendations took 2 main forms: (1) an independent privacy and security governing body and (2) a privacy and security subcommittee that is part of a larger governing body (other subcommittees might include technology, communications, and finance).

California has created a new independent privacy and security body, the California Privacy and Security Board. It was established to provide a governance structure to facilitate and guide the considerable amount of regional health information organization activity in California. The mission of the board is to establish security standards, develop privacy principles and policies, and, in general, continue the privacy and security efforts begun under the project. The board has established 4 committees: the Privacy Committee, the IT Security Committee, the Legal Committee, and the Education Committee.

Other states are also considering creating independent privacy and security bodies, particularly states in which the designated HIE has been given control over privacy and security issues. Some stakeholders have expressed concern about the independence of a privacy and security committee that is under HIE governance (this governance arrangement is now in place or being planned in 8 states). Two states noted that a governance arrangement in which the HIE oversees all aspects of governance could be interpreted as a conflict of interest, because the HIE is responsible for making financial decisions that might conflict with its need to uphold community standards for privacy and security. For example, Vermont noted that it had observed a healthy tension between the board of directors of Vermont Information Technology Leaders, the state's HIE, and some of the proposals emerging from the state's Privacy and Security Solutions project work. The concern about the independence of the HIEs is most prevalent in states that have only 1 HIE. As mentioned, California has already created an independent body to address the coordination of its nearly 30 HIE initiatives. Indiana and Massachusetts, which are in more advanced stages of development, did not see an immediate need for a new governance structure.

Governance bodies are in various stages of development in 13 states. Those in development are often emerging from new executive orders or legislation, although some are being explored without this support. The process is similar across states: (1) establish the body's authority and scope (by executive order or legislation), (2) create the body, (3) establish bylaws and operating procedures for the body, and (4) begin work. State teams are working in different stages of this process to determine the scope of the governance body, its membership, and its operating procedures. To ensure buy-in and respect for the body once it is established and implemented, state teams are actively seeking stakeholder input as they work through this process.

In addition, 4 state teams (Maine, Massachusetts, Puerto Rico, and Wisconsin) reported de facto governance in their state. For example, in Wisconsin, the Department of Health has

statutory authority over key privacy issues, and other players in the state also contribute to the development of policies and education of stakeholders. In Puerto Rico, the Department of Health has informal control over policy development. Maine and Massachusetts have convenor organizations that, although not the arbiters of privacy and security issues, bring stakeholders together to help develop consensus-based solutions.

Four states explicitly noted that they are not working toward the development of a privacy and security body. In New Hampshire, no HIE exists, and the state has determined that a privacy and security governance body is currently unnecessary. However, New Hampshire's Citizen's Health Initiative serves as a venue for continued privacy and security discussions. Two states (Indiana and Massachusetts) are in a more advanced state of development and judge that current practices and leadership are serving the state well. Massachusetts noted that a privacy and security governing body may be necessary in the future but not at this time.

As a result of state teams' desire to achieve support and respect for the governing body, the governance structures are not yet fully developed in the states, and their responsibilities are still being defined. Four states noted that, before the project, privacy and security were often taboo issues that stakeholders were quick to eschew as too difficult or contentious. As a result of the project, recognition is increasing in all participating states that privacy and security are essential components of any information exchange and that, even though the issues are challenging, consensus is achievable. This discovery arose from state teams' ability to reach additional and new stakeholders, an ability that itself was fostered by the Privacy and Security Solutions project. Moreover, 3 teams noted that the structure of the project (identifying variations, creating solutions, and implementing those solutions) helped create a shared understanding of privacy and security and directly supported the new and continuing governance of health information exchange.

The Privacy and Security Solutions project has also proved significant in its reach. Many state teams reported much higher levels of interest from governors, legislators, and state agencies than existed before the project. This reported increase in interest is supported by the increase in the number of bills and executive orders related to health IT and health information exchange that were introduced during the contract span.

## **2.4 Stakeholder Education and Knowledge**

One of the key goals of the Privacy and Security Solutions project was for state teams to create a broad base of support among stakeholders in their states to develop consensus solutions and sustainability that would extend beyond the contract period. The Privacy and Security Solutions project provided state teams with the resources to engage a broader range of stakeholders than would have been possible otherwise. Similarly, it afforded states the resources to engage on a broader array of issues. The following paragraphs describe

some of the additional stakeholder groups that teams have been able to involve and the implications of doing so.

State teams were able to engage a wide range of new stakeholders and tackle several challenging issues. Engagement with behavioral health providers and advocates has been key for states as they work to examine exchanges that are covered by the 42 C.F.R. pt. 2 regulations. For example, Massachusetts held a conference dedicated to examining the possible integration of mental and physical health records. Patients and advocates communicated that they often feel that mental and behavioral health records should be afforded higher levels of protection than they receive under the 42 C.F.R. pt. 2 requirements. Thus, meeting with both providers and advocates has helped the state understand the exchange landscape in greater detail and has informed future work.

Community health centers and rural home health practitioners were among the stakeholder groups that state teams engaged as a result of the project. These 2 groups often help disadvantaged or underserved communities. Thus, working with these stakeholder groups will help ensure that the benefits of the project are extended to historically disadvantaged communities.

States have also forged greater connections with state agencies that participate in or contribute to health information exchange, including state Medicaid and State Children's Health Insurance Program agencies, public health authorities, correctional facilities, and emergency management departments. Engaging with other agencies enhances the agencies' ability to exchange health information when needed, and to clarify roles and communication. In addition, state teams also engaged with professional organizations such as the American Health Information Management Association and the Health Information and Management Systems Society and other nationwide initiatives such as the Nationwide Health Information Network trial implementations and the National Governors Association State Alliance for e-Health. As states advance toward interoperable exchange, interfacing with other local and national initiatives will be a key to success.

To further understand the legal landscape, state teams have engaged with tribal nations to understand tribal laws and how exchange could be accomplished. Similarly, they have met with educational institutions to review the limitations of exchange imposed by the Family Education Rights and Privacy Act. By expanding the range of stakeholders that were included, state teams have created foundational support for continued work.

The project helped the state teams identify the need for education, which many stakeholders received as a benefit from the Phase I work. Education is now becoming formalized so that state teams can expand their reach and education of stakeholders. State teams are developing formal educational campaigns that will include publications, public service announcements, public forums, and websites. This work will be addressed across

states in the provider education and consumer engagement collaboratives, which are discussed in greater detail in Section 3.

The project has altered the opinions of state team members and stakeholders about privacy and security, as reported by the state project teams and evidenced by the diversity of stakeholder representation. Previously, these issues were often viewed as being administratively challenging and contentious and so were not directly addressed. As a result of the project, privacy and security are now seen as fundamental components of exchange that benefit all parties. In addition, teams and stakeholders now recognize that technology cannot be used to resolve all privacy and security issues. Instead, policies that support privacy and security must be developed, tested, and implemented. Understanding the intersection of policy and technology and how technology can support, rather than drive, policy has enabled the state teams to make rapid progress.

Overall, the Privacy and Security Solutions project has provided states with the “activation energy” that was required to engage stakeholders. State teams have repeatedly remarked on the momentum that has been built around health information exchange, as well as the project’s ability to drive new work. Early engagement with stakeholders has enabled and supported the implementation work that is under way; state teams expect that it will benefit new work in 2008 and beyond.

## **2.5 Development and Sustainability of Health IT/HIE Efforts in the States**

The Privacy and Security Solutions project has helped states establish a privacy and security foundation with which to develop new health IT efforts. Moreover, state teams have reported increased engagement of stakeholders in the development and continuation of health IT efforts. As the state teams develop privacy and security solutions and implement them, they decrease barriers for other health IT and HIE efforts. This is supported by the progress of existing HIEs towards higher levels of development, and fostered the development of new HIEs.

Fourteen states indicated that the Privacy and Security Solutions project has increased support for upcoming HIEs. In some states, HIEs were already in the development process when the project began; in others, they are just emerging. In states where the development process had already begun, the project provided clarity and focus. For example, 1 state team explained that the original consent model for the state’s HIE was an opt-out model (patients had to specifically request that their information not be included in the exchange). Through stakeholder engagement and feedback, the team shifted its focus and is now working with a much stricter opt-in model (patients must give permission for their information to be included in the exchange). Originally, this kind of model was dismissed as administratively undesirable and technically challenging. However, the input from the stakeholder community was clear, and the team began searching for technological

solutions that would support the stricter opt-in model. Seeking and incorporating stakeholder viewpoints has greatly supported state teams in their efforts to advance health information exchange. In states where HIEs are just beginning, the project has demonstrated that privacy and security can be addressed, even across stakeholder groups with seemingly disparate interests, as evidenced by their willingness to participate in the Privacy and Security Solutions project.

State teams also noted the timeliness of the Privacy and Security Solutions project. In several states, e-health initiatives were just beginning to emerge, and the project provided a vehicle for the work required in the state. Other state teams had no coordinated efforts for health IT. Again, the formalized processes of the project (identification of variations, development of solutions, and implementation of solutions) enabled the state teams to engage a wide range of stakeholders and to fully educate them about the centrality of privacy and security in health information exchange.

Twenty-three states referenced increased awareness of privacy and security issues among stakeholders as a key component of success in the development and sustainability of health IT and health information exchange. Several were surprised by the level of engagement among the stakeholder community. One state noted that stakeholders were relieved to hear that the project team was grappling with privacy and security issues, because the stakeholders had been hesitant to do so on their own. Four states remarked that the Privacy and Security Solutions project offered the first real forum for discussing privacy and security issues and that, for the first time, stakeholders were willing to engage because they felt secure in the process. Ten states indicated that collaboration has been significantly enhanced as a result of the project and that stakeholders are now better prepared to move forward and are planning for new opportunities and future implementation steps. Although much work remains, state teams have both directly and indirectly supported the development and sustainability of health IT and health information exchange.

### **3. COLLABORATIVE (CROSS-STATE) OUTCOMES**

Almost unanimously, states reported that working with 33 other states and territories on the Privacy and Security Solutions project proved extremely valuable toward understanding their state-specific challenges for health information technology (health IT) and health information exchange within a larger nationwide framework. In some cases, the benefits of simply being connected to one another under the same initiative were tangible. Alaska, Arkansas, Colorado, Connecticut, Kansas, Kentucky, Maine, Michigan, New Hampshire, New York, Washington, and West Virginia reported that interacting with other states during the activities hosted by RTI International, such as regional meetings, provided them with a sense of how they compared with other states in their progress on privacy and security issues and inspired them to address major roadblocks. One state reported that the cross-state, collaborative nature of the project had “put them in a place where they are more involved and aware of work being done in other states.”

A number of states reported that they are eagerly looking forward to continuing and deepening the connections with other states. Alaska, Colorado, Illinois, Indiana, Kansas, Mississippi, and Wisconsin stated that they anticipate devoting more time to cross-state collaboration after having focused most of the effort within their states during the first phase of the project. As 1 state reported, the project “has brought up the importance of [working across states]. We’d like to do more of it.”

The relationships that the states have forged, or are planning on pursuing, reflect a variety of cross-state interests. A number of states have established better communications with states in their geographical area. For example, Louisiana and Mississippi formed the Gulf Coast Task Force to address interoperability issues. Many states, however, have developed relationships that are based not on geographical proximity but on shared interests. Some states need to share health information with distant states because their citizens travel between them for vacations or health care. Alaska, for example, plans to expand discussions with California and Minnesota because these states are often visited by Alaskans for health care. Other states have formed relationships to share information about common approaches to health information exchange architecture, issues, or projects. For example, Mississippi and Wyoming are working together because both are developing web-based tools to educate parties in their states about privacy and security issues, and they want to minimize duplication of effort.

#### **3.1 Collaborative Work Groups**

To increase the focus on cross-state collaboration, RTI was tasked with coordinating and overseeing the formulation of multistate, collaborative work groups during the extension period (June through December 2007) of the Privacy and Security Solutions project. A

number of states (Arizona, Arkansas, California, Colorado, Connecticut, Florida, Minnesota, New York, Oklahoma, West Virginia, and Wisconsin) reported that the collaborative effort organized by RTI provided a source of interaction among states involved in the project that was defined and focused in a way that they had not previously experienced. More than one of these states reported being pressed for time to reach out to other states, even though the interactions were remarkably helpful: “The requirement to come together enables those connections.”

To begin the coordination of the collaborative work groups, RTI asked the 34 original Privacy and Security Solutions state project teams to submit a summary of the issues that required focused resolution in their states. Across these summaries, some common issues emerged. A meeting held in June 2007 brought together the project leaders from the 34 state teams to hold initial discussions about these common issues and the possible formulation of collaborative groups. Between June and September, discussions continued among the states, and RTI hosted web seminars to clarify the issues that would be of greatest worth to states participating in the collaboration. In addition, RTI worked with the National Governors Association to reach out to all states and territories that were not subcontracted to engage in the first phase of the project. These efforts produced an interested response from 16 states or territories (Alabama, Delaware, Georgia, Guam, Idaho, Maryland, Missouri, Nebraska, North Dakota, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Virginia, and Washington, DC).

In September 2007, RTI convened a meeting to solidify the membership, purpose, and objectives of each collaborative work group. This meeting was attended by representatives from 45 states and territories. Out of this meeting, 6 distinct collaborative groups were formed, 1 of which later divided into 2 groups focused on separate potential projects. The final 7 groups are discussed in the following paragraphs.

### ***3.1.1 Consumer Education and Engagement***

The mission of this collaborative work group is to develop a process that increases the targeted consumer-population subgroups’ engagement in and understanding of privacy and security issues in health information exchange. Each state will contribute materials that have proven effective in various situations for a toolkit that can be used by a wide variety of entities to educate and engage consumers in the privacy and security of their health records. Participating states are as follows:

- Colorado
- Georgia
- Kansas
- Massachusetts
- New York
- Oregon
- Washington
- West Virginia

### **3.1.2 Provider Education**

The mission of the provider education collaborative is to develop tools and techniques to enhance provider awareness, inform and motivate, and engage providers in adopting and using electronic health information exchange in a secure and private manner. Existing health information exchange initiatives have noted that the preponderance of provider concerns in this arena tend to be centralized around issues of access to health information, security of patient and provider information, and the implications for provider liability. This work will help to reduce or eliminate barriers to the interoperable exchange of health information identified during the previous Privacy and Security Solutions project phase (such as differing interpretations of the Health Insurance Portability and Accountability Act [HIPAA] and state laws and the perceived privacy and security dangers of interoperability), which will in turn create local and regional “physician champions,” who have proven to be a key resource for the acceleration of health information exchange adoption. Participating states are as follows:

- Florida
- Michigan
- Tennessee
- Kentucky
- Mississippi
- Wyoming
- Louisiana
- Missouri

### **3.1.3 Standards Policy Adoption**

The mission of this collaborative work group is to establish draft business or operational security policies/practices that can be tied to already proposed technical standards. The collaborative will explore differences in the concept, design, and business models for health information exchange in various states and their implications for varying health care privacy and security practices. Once these are articulated, the group will seek to define HIPAA-compliant minimum business or operational policies/practices by which these HIEs may share information across state lines. Participating states are:

- Arizona
- Nebraska
- Virginia
- Colorado
- Ohio
- Washington
- Connecticut
- Oklahoma
- Maryland
- Utah

### **3.1.4 Harmonizing State Privacy Law**

This collaborative work group plans to create and pilot a legislative template, with a common taxonomy, which will allow each state to analyze its own privacy and security laws and better understand the requirements for health information exchange within and across state lines. The collaborative seeks to increase stakeholder awareness and understanding of the state laws governing health information exchange. Additionally, the legislative template

will help enable consensus in the interpretation of such laws. Participating states are as follows:

- Florida
- Idaho
- Kansas
- Kentucky
- Michigan
- Missouri
- New Mexico
- Texas

### ***3.1.5 Consent Options, Outcomes, and Best Practices***

The mission of the collaborative on consent strategies is to develop resources for entities attempting to make decisions about consent process and policy. The collaborative will recommend approaches to obtaining patient consent for release of information, both within states and between states. Such a strategy needs to begin locally but coordinate with national efforts addressing consent. All states will be able to use the tools and decision-making tactics developed by this collaborative to make informed choices regarding their strategies for obtaining consent to exchange information. Participating states are as follows<sup>8</sup>:

- California
- Illinois
- North Carolina
- Ohio

### ***3.1.6 Consent Data Elements Required for Data Transfer***

The mission of this collaborative is to understand the landscape of electronic consent between states. States participating in this collaborative will identify the commonalities and/or differences in what is required to release patient medical information across state lines, and to identify possible solutions to facilitate interstate health information exchange. This project seeks to reduce the effort required to support the capability for interoperable clinical data exchange across states for specifically identified patient clinical situations and recognizes the need to better understand the capabilities of each state to use and disclose protected health information before interstate health information exchange can begin.

Participating states are as follows:

- Arkansas
- Indiana
- Maine
- Massachusetts
- Minnesota
- New Hampshire
- New York
- Oklahoma
- Rhode Island
- Utah
- Vermont
- Wisconsin

---

<sup>8</sup> Arizona, Kentucky, New Jersey, and West Virginia will review core team products.

### 3.1.7 Interorganizational Agreements

The mission of this collaborative is to develop model cross-state interorganizational agreements, such as memoranda of understanding (MOUs) and data-sharing agreements, that will provide the participating states and territories and related departments and entities, and the providers within those states and territories, with the ability to conduct interoperable health information exchanges. Fine-tuning the privacy and security components of the agreements will be the primary focus.

Participating states and US territories are as follows:

- Alaska
- New Jersey
- Puerto Rico
- Guam
- North Carolina
- South Dakota
- Iowa
- North Dakota

### 3.2 Other Cross-State Initiatives and Interstate Projects

In addition to the formal multistate collaborative groups formed under the Privacy and Security Solutions project, a number of states have reported laying foundations for or undertaking cross-state projects as part of the Privacy and Security Solutions project work. Some of these cross-state interactions resulted from networking opportunities provided by the project. Many states were able to point to distinct instances in which discussions with other states served as a significant resource informing their own projects:

- Massachusetts was able to ask other New England participants for information on consumer engagement.
- Mississippi and Wyoming engaged their teams in combined discussions about web-based tools and exchanged resources to minimize duplication of effort.
- New Hampshire engaged in discussions with Colorado about the impact of and issues associated with consent.
- New York coordinated with Massachusetts to gather information about consent protocols.
- Alaska, Oregon, and Washington strengthened the connection between the northwestern states, finding similarities in their populations and proposed initiatives. They continue to meet as necessary to discuss ideas to move forward collectively.
- Ohio developed a permission form that Minnesota, Missouri, New Jersey, Pennsylvania, West Virginia, and Wyoming have expressed interest in using; discussions continue on the possible adoption of a common version of the form.
- Arizona, Connecticut, Florida, and Indiana reported frequent and helpful interactions with a number of states participating in the project.

“As needed” access to a network of individuals from multiple states working on similar issues proved to be a great asset to these state teams. As 1 team noted, the project created “a lot of interest from neighboring states about breaking down barriers to

exchanging data,” producing “a lot of inroads and off-line conversations between state agencies.” Throughout the project, many of these connections were solidified into formal multistate initiatives:

- Florida, Louisiana, Minnesota, Mississippi, and Oklahoma established regular conference calls to discuss the common issues experienced on the project and to share ideas on moving forward.
- Indiana created a multistate committee to explore ways to resolve the 42 C.F.R. pt. 2 drug and alcohol abuse treatment information-consent issues facing HIEs today and to work on developing a model for electronically implementing the consent process. Response to this committee has been strong, and the initiative has held preliminary meetings with the Substance Abuse and Mental Health Services Administration to discuss the committee’s ideas and recommendations. States actively involved include Arkansas, California, Indiana, Louisiana, Maine, Massachusetts, Michigan, Minnesota, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, Utah, Washington, and Wisconsin.
- New Jersey and New York worked together to conjoin the immunization registries of New Jersey, New York State, and New York City. Each entity is working on core issues, such as identification of individuals, feasibility of data sharing, and establishment of a memorandum of understanding. New Jersey has also communicated with other participants, such as Florida and Puerto Rico, about plans to expand this initiative.
- Iowa and Nebraska are discussing a pilot exchange of data between the Iowa statewide Immunization Registry Information System (IRIS) and the Nebraska electronic registry system. Work is under way to enhance the exchange capabilities of IRIS with electronic health record systems for private practitioners and schools. These initiatives currently take precedence, but initial discussions continue to lay the groundwork for moving forward on this initiative.

The potential for multistate and cross-collaborative work between the states is exceptionally strong, especially given the foundation that has been provided by the Privacy and Security Solutions project. Early in the project, participants worried that 1 initiative among all the states would be insufficient or unhelpful in moving them toward interstate electronic health information exchange. During the final stages of the extension phase, project teams indicated that their primary reason for not engaging in more multistate activity was simply the demands of other project work. Although states have various levels of preparation for and continuing work toward intrastate electronic health information exchange, most participants are interested in working with other states to create common solutions. One state team reported that the project “introduced [it] to a whole new group of people in other states that have a lot of information to share.” Another team predicted that “the future is certainly going to be all the states working together toward some common causes.”

## 4. OVERVIEW OF INDIVIDUAL STATES/TERRITORIES

### 4.1 Introduction to the Individual State/Territory Overviews

This section summarizes the impact of the Privacy and Security Solutions project on the individual states participating in the project. Participating states are presented in alphabetical order. Each state's report includes 3 sections. The first section, "Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project," describes the status of electronic health information exchange that existed before the project began. These descriptions have been drawn primarily from the proposals submitted by each state to be part of the project. The intent of this section is to provide the context for understanding the impact of the project and describe the particular challenges faced in each state related to factors such as geography, population, and the health care delivery system. The second section, "Current Health IT/HIE Landscape," captures changes in the landscape that have occurred since those proposals were submitted, drawn from project reports on activities in each state, review of websites and other available material, and verified in discussions with key project staff in each state. The section describes progress made toward exchanging health information, such as the development of regional health information organizations (RHIOs) or similar entities, or efforts to expand the exchange of health information. The third section for each state, "Current Privacy and Security Landscape," focuses on the project's impacts within each state on furthering privacy and security within the context of electronic health information exchange. This section was also drawn primarily from project reports and discussions with key project staff.

#### 4.1.1 Alaska

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Although Alaska has a small population living in a large geographical area, this population has had consistent collaboration among health care partners and competitors working on progressive health information technology (health IT) and health information exchange projects. Before the Privacy and Security Solutions project, prior efforts had pointed to a need to improve health care quality through more efficient health information exchange in Alaska. This need is documented in numerous statewide assessment reports, including the *Evolution and Summative Evaluation of the Alaska Federal Health Care Access Network (AFHCAN) Telemedicine Project*, the Alaska Telehealth Advisory Legal Subgroup report, the Alaska Department of Health and Social Services report titled *Public Health Information Network (PHIN) Readiness Assessment*, and Alaska 20/20.

Alaska has a long history of implementing information technology to overcome its geographic environment. The most prominent and progressive health IT project has been

the AFHCAN “store and forward” telemedicine system, which at the time of the proposal was used at more than 250 federal and state sites. Additionally, the Alaska Tribal Health System, a collaborative of 39 autonomous tribal health organizations, has run an integrated network exchanging health information data on Indian Health Service clients since 1994. The US Department of Veterans Affairs operates a similar system in Alaska for veterans’ health information.

The Alaska Federal Health Care Partnership was founded in August 1995 to establish and take advantage of collaborative efforts, including training, service contracts, and technology. The Alaska Telehealth Advisory Commission was formed in 1998 to coordinate health IT activities and provide a forum for health care organizations that would assist in closer collaboration of telehealth activities. The commission changed its name to the Alaska Telehealth Advisory Council in 2000 and re-formed as Alaska ChartLink in 2005. The Alaska Electronic Health Record (EHR) Alliance was formed in 2005 to support the implementation of electronic health records (EHRs) in physician offices in Alaska.

### *Current Health IT/HIE Landscape*

Alaska ChartLink remains the major, central initiative in the state. However, the project team is quick to add that the Privacy and Security Solutions project allowed them to interact with new stakeholders. It enabled the groups to devote time to thinking through some of the looming issues and to conduct conversations necessary to moving forward with ChartLink in a statewide HIE.

The state is establishing a formal governance structure to address issues such as privacy and security. Currently, everything filters through ChartLink. Although Alaska cannot report any new health IT/health information exchange initiatives at this time, the consensus is that the Privacy and Security Solutions project injected energy into the ongoing initiative of health information exchange, and efforts are under way to secure additional project funding.

Through regional and national meetings, the Alaska project team was exposed to interstate issues in the development of electronic health information exchange. Although efforts remain focused on the many challenges of health information exchange within the state, the project team has established firm contacts with counterparts in other states, in particular Oregon and Washington.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project has resulted in a nucleus of individuals who have become knowledgeable about current practices in the state and where best to implement change to encourage electronic health information exchange while preserving protection of health information. In Phase I of the Privacy and Security Solutions project, an assessment of the current privacy and security landscape in Alaska was completed. This assessment included an intensive investigation of current community practices and the legal

environment. More than 250 Alaska citizens from across the state volunteered in stakeholder meetings held in both urban and rural locations. Barriers to interoperable electronic health information exchange and solutions that preserve privacy and security were identified and categorized by stakeholder workgroups.

Based on the work of these groups, a set of best possible solutions to facilitate the use of health information exchange and EHRs in Alaska was developed. The results were 4 broad categories: Legal Solutions, Standardization of Policies and Procedures, Participant Agreements, and Education and Marketing. After reviewing each of these categories with relevant stakeholders to determine the necessary steps to reduce barriers, the Alaska Core Team and steering committee selected 2 recommended solutions. These include drafting documents and procedures necessary to begin data sharing and to develop a communications plan and pilot a limited marketing campaign.

Efforts are taking place to establish a formal governance structure for privacy and security in Alaska. Alaska ChartLink, formed in December 2005, is spearheading the effort to promote widespread access to a private and secure statewide data exchange. Participation in the Privacy and Security Solutions project has informed and helped coordinate these efforts. Access to information about EHR projects in other states has also informed Alaska's ongoing implementation efforts. The consent documents being developed in Phase II of the Privacy and Security Solutions project are being used to inform the privacy and security policy of ChartLink.

Based on an initial review of the documents listed in the Privacy and Security Solutions project Phase I Final Report, the Core Team selected 5 documents that were drafted and reviewed for implementation by Alaska ChartLink:

1. Privacy and Confidentiality Policy
2. Policy and Procedure for Addressing Breaches of Confidentiality
3. Identification and Authorization Policy
4. Provider Participation Agreement
5. Patient Participation Agreement

In drafting these policies, the steering committee was aware of already existing policies and procedures at each organization and determined that it was best not to impose detailed instructions that may conflict with those policies. Instead, each document was set up to provide a minimum floor that each provider must meet, and allows the provider to adopt more stringent policies as desired.

Prior to the Privacy and Security Solutions project, Alaska had no coordinated statewide approach to addressing issues of privacy and security. The project has filled this gap by

developing standardized policies, procedures, and participation agreements. The assessment of variations in business practices and policies and the policies, documents and educational materials developed during the project will be utilized to assist in implementing the business plan for Alaska ChartLink.

The collaborative process initiated by the Privacy and Security Solutions project facilitated the exchange of ideas and lessons learned between many states. Based on diverse stakeholder participation, the project team in Alaska developed “best practice” solutions to privacy and security issues. The project has created an opportunity for Alaska to advance the health information exchange and EHR initiatives within Alaska and has opened the door to potential future grant opportunities.

#### **4.1.2 Arizona**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

On August 30, 2005, Governor Napolitano issued an executive order to develop Arizona Health-e Connection. Under the order, a steering committee was charged with developing a road map by which Arizona can achieve statewide electronic health data exchange among insurance companies, health care providers, and consumers of health care. Additionally, the committee is exploring issues related to the implementation of EHRs. To assist the steering committee, the governor established 5 task groups (governance, financial, clinical, technology, and legal) charged with making recommendations in their respective areas of expertise to facilitate the creation of a statewide electronic health information exchange system and to encourage migration to EHRs.

When Arizona submitted its Privacy and Security Solutions project proposal, various entities in Arizona were working on health IT and health information exchange projects, including the following:

- Arizona Department of Health Services Electronic Disease Surveillance Program
- Arizona Telemedicine Program
- Health Services Advisory Group (Arizona’s Medicare Quality Improvement Organization) Doctor’s Office Quality-Information Technology (DOQ-IT) program
- Arizona State Immunization Information System
- Arizona Health Information Technology Accelerator and Arizona Medical Associations
- Southern Arizona Uninsured Coalition, which developed the Southern Arizona Health Information Exchange (SAHIE) project
- Arizona Health Query, a longitudinal database at Arizona State University that is used for health services research
- EHRs used by many Arizona hospitals and some Arizona physicians

However, the state lacked a unified vision of how to achieve greater adoption of health IT and a health information exchange system.

### *Current Health IT/HIE Landscape*

Arizona Health-e Connection received the Council of State Governments' 2007 Innovation Award for best practices in promoting health IT adoption in the state. Arizona Health-e Connection's role is threefold: (1) serving as an educational resource and information clearinghouse for electronic health information exchange initiatives throughout the state; (2) serving as a voluntary standards- and rules-setting body to coordinate and foster health information exchange activities throughout the state; and (3) building infrastructure, where appropriate at the state level, to support statewide initiatives, foster efficiency, and limit duplication of resources. The state team cites the legal work and the organization's ability to promote privacy and security surrounding electronic health information exchange as one of the most tangible outcomes of the Privacy and Security Solutions project.

Arizona Health-e Connection is actively supporting 2 HIE initiatives in Arizona: (1) the development of the Southern Arizona Health Information Exchange and (2) the Arizona Health Care Cost Containment System (AHCCCS)—Arizona's Medicaid agency—in its work to create an HIE under a Medicaid Transformation Grant of \$12 million. The health IT/health information exchange atmosphere in Arizona is positive, supported by the governor's office, collaborative, and energized.

In 2007, the Rural Health Information Technology Adoption Grant program was established in Arizona. Funding of \$1.5 million was received by the Arizona Government Information Technology Agency to provide grants to promote health IT/health information exchange adoption in the rural areas. The recipients of the grant included 3 community health centers, 3 hospitals with partners, and 1 behavioral health center. This program has affected 178710 patients and 325 rural providers.

The Rural Health Information Technology Adoption grant was subsequently funded for \$1.5 million for each of fiscal years 2008 and 2009. These funds will be used to support the development of RHIOs in the rural communities, provide funding to survey the rural communities about their use of health information exchange, and award funds for rural communities to receive project management training.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project in Arizona has been fundamental to the Legal Work Group (LWG ) of the Arizona Health-e Connection, a voluntary standards-and rules-setting body that now coordinates health information exchange activities throughout the state. The model privacy and security policies for health information exchange and the model participation agreement, current under development by the Arizona Health-e Connection's LWG, are based on the work of the Privacy and Security Solutions project.

These model policies and agreement will be used by HIEs throughout the state, including the SAHIE and AHCCCS projects. Standardized approaches to privacy and security in Arizona HIEs are essential to achieve “policy interoperability”—the ability for Arizona HIEs to communicate with one another. The LWG is also working on statutory and regulatory changes to assist in the implementation of HIEs in Arizona. The LWG has identified statutes and regulations—many of which were penned in an era of paper medical records—that are barriers to the implementation of HIEs. In addition, the LWG is working on an enforcement framework for HIEs to ensure that they operate in a manner that protects the privacy and security of individuals’ health information with real accountability. Participation in the Privacy and Security Solutions project has allowed Arizona team members to engage previously overlooked stakeholder groups, such as long-term health care providers, consumers, consumer advocacy groups, and tribal health organizations, in the consideration of privacy and security issues.

Arizona is collaborating on health information exchange with several other states, including Oregon, Utah, and Washington. The multistate collaborative will be analyzing policies on authentication, access, authorization, and audit for interoperable health information exchange among the states.

During the Privacy and Security Solutions project, the project team developed an authentication and access approach for providers to access an HIE. They researched national standards for authentication and conducted interviews with existing HIEs to learn about their approaches to authentication. The project’s LWG identified and began work on removing barriers to exchange of data in the areas of communicable disease, mental health, immunization and genetic testing through statutory amendment. They also developed a comprehensive enforcement and consumer rights framework. The project team continues to involve a large number of stakeholders in the planning and development of health information exchange capacity in Arizona.

The Privacy and Security Solutions project conducted several individual meetings with major stakeholders in Arizona to communicate the proposed process requirements and discuss methods of authenticating providers and assigning access to private networks and electronic medical records systems. In addition, they reported progress monthly to the executive and the clinical/technical committees of the Arizona Health-e Connection. As a result, the project team identified the need for continued work in the following areas:

- Develop a method in the community to achieve single sign-on for providers. This is a challenge because many applications may be used at different participating entities, requiring several different logins and passwords (even within one institution).
- Develop an electronic method for listing authorized users from participating entities in the HIE directory of providers. Automating this process might be costly and add extra burden on IT departments.

- Work closely with hospitals, community health centers, and other health care organizations to develop the trust necessary for these providers to allow the HIE to obtain a list of authorized users electronically.
- Conduct future research on the cost of using tokens, biometrics, and digital signatures to authenticate users, as well as public key infrastructure (PKI).
- Work on how to authenticate providers who are not affiliated with participating entities (such as physicians who do not have medical staff privileges at a hospital).
- Develop techniques to authenticate individuals who are not licensed health care providers or not affiliated with a participating entity, if an HIE wants to provide access to individuals.

The Privacy and Security Solutions project in Arizona identified the need to make the health information exchange registration process easy for providers, leveraging the existing organizations that credential, identify, and authenticate providers. Additionally, consumer communication has been identified as critical in conveying an explanation of these methods to consumers to build trust among consumers about sharing electronic health information.

The project's LWG has developed a comprehensive package of proposed statutory and regulatory amendments for health information exchanges, a model participation agreement, and a model set of policies and procedures for nascent exchanges in Arizona. They have involved a wide range of stakeholders in the legal work and expect their analyses and materials to achieve wide acceptance in the community.

Their priorities for building on this work in 2008 include outreach and education to consumers, providers, and the Arizona legislature to continue to raise awareness of health information exchange and the need for the proposed statutory and regulatory amendments. If the legislative package is introduced in January 2009, a substantial amount of work will occur in the last quarter of 2008, through the first half of 2009, to shepherd the proposed statutory amendments through the Arizona legislature.

In 2008, they also plan to revisit the model participation agreement and model policies and procedures for health information exchange, as the HIE initiatives develop concrete architecture plans. This will need to be an evolving set of documents to be responsive to the needs of Arizona HIEs.

An outcome of the Privacy and Security Solutions project work is that the project team has developed a real community concerned about general issues related to health IT and specific concerns related to privacy and security of health information. Six discrete organizations interact regularly with one another, share information, and are linked into a larger group of some 200 organizations, including consumer organizations, tribal communities, hospitals, health care providers, and others. Arizona Health-e Connection reports a "massive amount of volunteer involvement."

Recognition of the challenges of wider outreach to consumers has led to the development of the Arizona Health-e Connection Consumer Advisory Council. Utilizing feedback from consumers and a wide array of providers, they will resolve important policy decisions on health information exchange, particularly whether and how consumer consent will be sought to include information in the health information exchange.

### **4.1.3 Arkansas**

#### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

The US Census considered Arkansas to be one of the least “wired” states in the United States, with limited Internet access in many areas. The Health Resources and Services Administration (HRSA) designated many communities in Arkansas as medically underserved regions. The lack of health services manpower also limited the availability of human resources to effect health IT adoption. Arkansas has a high rate of solo physician practices, which often lack resources to bear the cost of transition from paper to electronic systems.

The main health IT/health information exchange initiative in Arkansas in March 2006 was the DOQ-IT project, funded by the Centers for Medicare & Medicaid Services (CMS). The objective of the DOQ-IT project was to support the adoption and effective use of health IT by physicians’ offices to improve the quality and safety of health care. Arkansas was able to enroll more than 400 physicians and 150 clinics into the DOQ-IT program, which exceeded its recruitment goal. Other than the DOQ-IT program, all health IT/health information exchange efforts in the state were at the hospital level. Before the Privacy and Security Solutions project, these efforts were fragmented, with little or no cohesiveness or coordination.

#### *Current Health IT/HIE Landscape*

The eHealth Initiative is funding the Arkansas Foundation for Medical Care (AFMC), which is the quality improvement organization for the state. The AFMC is advancing the implementation of health information exchange in Arkansas by building on the state’s health information exchange experience as a DOQ-IT pilot state. Local stakeholders, such as the Arkansas Medical Society, Arkansas Hospital Association, Arkansas Health Care Association, HomeCare Association of Arkansas, Arkansas Department of Health and Human Services, Arkansas Pharmacists Association, Office of Long Term Care, Blue Cross Blue Shield, United Health, and QualChoice are working with AFMC to create a health information network. Through a grant from the Federal Communications Commission, Arkansas has been able to enhance the broadband infrastructure that will help make state health information exchange possible. Additionally, AFMC is exploring the feasibility of partnering with the state’s Medicaid program provider, the Arkansas Department of Health and Human Services, Division of Medical Services.

The Arkansas Delta Inpatient/Outpatient Quality Improvement project, led by St. Bernard's Medical Center, is a health IT project funded by the Agency for Healthcare Research and Quality (AHRQ). This initiative uses a computerized decision-support system, pharmacy information system software, Misys Insight (clinical real-time alerting software), and EHRs to accomplish the goal of improving quality of care and patient safety in the 23-county targeted service area. The initiative will take advantage of a preexisting IT system linking the medical center to the clinics. The project includes a training component for 260 physicians, 1000 front-line clinicians, and 257 students in nursing and other health professions. It also includes a hospital pharmacy component.

### *Current Privacy and Security Landscape*

Prior to the state's participation in the Privacy and Security Solutions project, the Arkansas privacy and security landscape was fragmented. Certain key entities were engaging in collaborative efforts, including the Arkansas Hospital Association, Arkansas Blue Cross and Blue Shield and through the previously described AFMC activity. The Privacy and Security Solutions project has both increased stakeholder engagement and strengthened the coordination of activities in the state, resulting in more comprehensive efforts.

The opportunity to participate in the project allowed Arkansas to examine variations in laws and business practices related to privacy and security of health information exchange. The Arkansas project team identified potential solutions for improving the status of electronic health information in the state through incorporation of interoperability standards and protocols. It is Arkansas' goal to sustain the project as a platform to facilitate ongoing efforts that will ultimately result in improved efficiencies and access to care, decreased medical errors, enhanced continuity of care, and reduction in escalating health care costs.

One of the deliverables for the Arkansas project team is a set of recommendations for a single, centralized entity for the governance of privacy and security issues in Arkansas. Efforts included reviewing activities undertaken by the Arkansas Hospital Association, Arkansas Blue Cross Shield and Blue Shield, and the AFMC. During the operation of the Arkansas Privacy and Security Solutions project, existing broader health information exchange and health IT efforts in Arkansas have become integrated within the AFMC. Privacy and Security Solutions project team members now serve on the steering committee and LWG for the AFMC, thus leveraging their project experience.

The AFMC will create a strategic plan for health information exchange and health IT efforts in Arkansas to be delivered in spring 2008. This plan is expected to include a recommendation for centralized oversight and coordination of health information exchange and health IT generally, specifically including privacy and security issues. The Privacy and Security Solutions project team in Arkansas will continue to work with AFMC staff and leadership to develop an efficient health information exchange and health IT oversight structure where privacy and security figure prominently.

Another goal of the Arkansas Privacy and Security Solutions project team is educating and encouraging the effective use of Arkansas-specific health law essentially related to privacy and security. To accomplish this goal, the Arkansas project team compiled existing information (primarily statutes from the Arkansas Code Annotated) into an Arkansas Health Information Privacy and Security Statutory Bench Book. The Bench Book will serve as a road map, detailing existence and location of statutes impacting electronic health information privacy and security in Arkansas. It is expected to become a quick and simple reference tool for organizations and individuals needing to understand a state-specific law that impacts electronic health information privacy and security in their business practices and patient transactions. While it will stand alone as a useful resource, the Bench Book will also serve as a base for the longer term vision to consolidate all privacy and security laws.

In the initial assessment of variations in business practices and policies, the Arkansas Privacy and Security Solutions project team found that understanding and application of state and federal HIPAA mandates and requirements are inconsistent. Testimony from stakeholders uncovered examples of both situations in which health information was released in ways that were less than HIPAA-compliant and, more commonly, situations where, though permitted by HIPAA, information was not shared because of unwarranted fear of penalty. Either situation resulted from a lack of clarity about the practical application of HIPAA.

To address this confusion, the Arkansas Privacy and Security Solutions project team developed a uniform, plain language-based HIPAA training course syllabus specifically tailored to privacy and security issues. The course is intended to address the need for a commonly shared and accurate understanding of privacy and security requirements. Consistency in application and understanding of HIPAA privacy and security mandates is essential to ensure patients, health care providers, and others interacting with the health care system are exchanging health information in the same safe and secure manner. This shared HIPAA training program is targeted at providers and other health care-related entities and is intended to minimize misunderstanding of what HIPAA does—and notably, what HIPAA *does not*—require with respect to patient privacy and security in electronic health information exchange. The training syllabus will be submitted to the Arkansas Department of Human Services to develop training material and utilized in the statewide HIPAA training. This training program will be replicable by other states to promote increased uniformity of perception and practice across states.

Arkansas project team members will staff to Governor Beebe's Roundtable on Health Care. The Arkansas Center for Health Improvement, an organization led by the Arkansas Surgeon General, was requested to establish the Roundtable to study health care issues in Arkansas and make recommendations for legislative and executive branch action. Participation by the Privacy and Security Solutions team will ensure integration of findings and recommendations of the project into broader health care system studies undertaken by the

Roundtable. A primary issue to be addressed is the lack of continuity of care and insufficient access to health care in the existing health care system, concerns that can be ameliorated through the employment of integrated health information exchange.

Arkansas reported that participation in the Privacy and Security Solutions project has generated numerous dividends for their state. The funding allowed them to create a common table at which disparate stakeholders convened to discuss issues related to privacy and security. As a result, one of the most important outcomes has been the increased awareness of health information exchange and health IT concerns in Arkansas. It not only solidified relationships with key stakeholders, but also stimulated Arkansas to engage additional stakeholders in the consideration of privacy and security issues—stakeholders that otherwise might have been left out.

The Privacy and Security Solutions project has encouraged collaboration with other states in formulating and implementing privacy and security solutions. While Arkansas historically has enjoyed good relationships with neighboring states such as Oklahoma and Mississippi, the project has helped the state establish relationships with other states, such as Indiana, Massachusetts, Minnesota, and Rhode Island, giving Arkansas access to knowledge and materials that would have been otherwise difficult to obtain.

Participation presented the opportunity for Arkansas to establish relationships with privacy and security experts who will facilitate effective collaboration on future projects. The Arkansas team members noted that the Privacy and Security Solutions project made them much more aware of the time, energy, and funding necessary to sustain these efforts. The project helped them “plant the seed,” and with the support of the governor, they are hopeful that Arkansas will be able to make additional progress in the near future.

#### **4.1.4 California**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

At the beginning of the Privacy and Security Solutions project, in March 2006, over 20 city, county, and regional HIE entities existed in California, and additional initiatives were under way, despite the state’s stringent privacy and security laws.

In 2005, industry leaders in California came together to form the California Regional Health Information Organization (CalRHIO) in an effort to bridge the gaps preventing interoperability. CalRHIO has brought industry representatives to the table to develop endorsed state interoperability standards, agree on the development of pilots for information exchange, and engage key stakeholders in developing the vision of information exchange in California. Even before the Privacy and Security Solutions project, progress toward building a statewide information exchange had been made in California through the efforts of CalRHIO and similar organizations, such as Health-e-LA. CalRHIO serves as an

umbrella organization that brings together health care stakeholders to develop common elements, such as governance, operational processes, technology, and financing, that are required for the formation of 1 or more RHIOs in the state.

HIE projects in California at the time of the Privacy and Security Solutions project proposal included several private and public entities exchanging health information electronically, but with little in the way of coordination among these programs.

### *Current Health IT/HIE Landscape*

Concurrent with the Privacy and Security Solutions project, California has continued to build on successful partnerships and collaborations as it works toward the goal of full interoperability and secure electronic health information exchange throughout the state. One of the newest entries in California is the Building Clinic Capacity for Quality program, which helps community clinics, community health centers, and consortia assess their capacity to participate in technology-enabled quality improvement. The program provides ways to help these organizations take a logical, stepping-stone approach to building their capacity for proceeding with this improvement.

Before joining the Privacy and Security Solutions project, California already had a significant start toward building interoperability in the state, with more than 20 different health IT/HIE initiatives. California now has 28 health IT/HIE initiatives, and 2 more under development. The environment for health IT and health information exchange in California remains positive and collaborative. One example is the progress made by the state's 2-year-old central RHIO, CalRHIO, toward achieving interoperability, including the following activities:

- delivering critical health information services reliably and affordably;
- creating a secure, electronically connected California;
- offering an information infrastructure that supports optimum care; and
- facilitating regional HIEs and interconnections among them.

### *Current Privacy and Security Landscape*

The statewide collaboration and engagement with stakeholders that occurred during the Privacy and Security Solutions project has become the foundation for the recently established California Privacy and Security Advisory Board (CalPSAB). It was established to provide a governance structure to facilitate and guide the privacy and security decisions faced by the designated RHIOs and other state government and education models in California. CalPSAB's mission is to establish security standards, develop privacy principles and policies, and, in general, continue the privacy and security efforts begun under the Privacy and Security Solutions project. The board has established 4 committees: the Privacy Committee, the IT Security Committee, the Legal Committee, and the Education Committee.

When California began to participate in the Privacy and Security Solutions project, very little collaboration existed between the private and government sectors of the state's health care industry. The first statewide private/public collaboration was established under the auspices of the project.

From the project's initial assessment of variations in business practices and policies, it was clear that an environment for health information exchange would require a formal collaborative process led by the state. In October of 2007, the Secretary of California Health Human Services Agency (CHHS) convened the first CalPSAB, composed of representatives from the major statewide health industry associations and government entities, and assigned the task to develop and recommend to the Secretary the privacy and security standards necessary to enable safe and secure health information exchange in California. Subsequently, 3 of its 4 committees held their first meetings: the privacy committee, the security committee, and the legal committee. The first meeting of the education committee will take place in January 2008.

As part of the process to implement the CalPSAB effort, the following tools were developed:

- An issue management process specific to privacy and security demonstrates the logical procedure to address the issues identified in Phase I of the Privacy and Security Solutions project and blends them with the areas of HIPAA that allow flexibility to entities.
- Initial project schedules allow appropriate and timely interaction as proposed solutions are developed between the committees and the board.
- Communication charts demonstrate the flow of communication among the many parties involved in supporting the CalPSAB and its committees.
- A flow chart illustrates the issue analysis flow, describing what steps are necessary to conduct a deliberative analysis of an issue.
- New forms support the issue analysis process document, a deliberative procedure of identifying, analyzing and proposing potential solutions, including implementation challenges. In addition, lists of criteria are provided that may be utilized to brainstorm alternative solutions and for weighing those alternatives.
- A description is provided of the communication suite established to enable transparent statewide discussions by the committees, task groups, and the CalPSAB.

The activities of the Board and its committees are expected to have significant impact on HIE efforts in California. Approximately 375 individuals receive information using the CalPSAB communications suite, 174 of whom participate either on the Board or its committees. These individuals come from throughout California and represent all categories of entities in the health care industry. A few individuals from other states are part of the interested parties who participate and/or elect to receive information.

The Privacy and Security Solutions project has been a catalyst for awareness of privacy and security issues in California and, in particular, the importance of collaborating with

consumers. Consumers recognize that advancements in technology alone are not sufficient to achieve interoperability. In terms of interstate and regional collaboration, California's Privacy and Security Solutions project efforts have been closely coordinated with New York's efforts. California anticipates sharing information about privacy policies and security standards with Oregon and Washington. California has also shared results with 16 other project states during the project.

#### **4.1.5 Colorado**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

During the summer of 2004, the Colorado Health Institute (CHI) convened a series of meetings with representatives from health care provider organizations, academic researchers, and community agencies involved in health IT projects to pursue a statewide vision for how this technology could improve the quality and cost-effectiveness of health care in Colorado. To set a baseline of information about current and promising projects and to discuss health information exchange and statewide health IT infrastructure development, CHI produced a white paper that identified and categorized the various health IT projects under way in the state and elsewhere.

In October 2004, AHRQ announced that Colorado, through its Colorado Health Information Exchange (COHIE) project, was one of 5 states awarded a \$5 million contract to develop a prototype for statewide interoperability through a clinical point of care health information exchange. The contract involved 4 major health care systems as project partners among whom exchange would be developed as part of a statewide health information network. These included Denver Health, a major safety net hospital and clinic system; Children's Hospital, a state and regional referral center; University Hospital, an academic teaching hospital; and Kaiser Permanente of the Colorado region.

During 2005, CHI facilitated multistakeholder consensus for the launch of a statewide Colorado RHIO, and an informal coalition coalesced as the Colorado Regional Health Information Organization (CORHIO) steering committee. With the goal of bring about statewide health information exchange by building on a federated clinical data exchange model, the CORHIO steering committee explored the design and implementation of CORHIO, including stakeholder health information exchange needs and interests, experiences in other states, and evolving issues regarding HIE development, including resources necessary to implement electronic health information exchange and economic sustainability of the technology's use.

Many stakeholders in the CORHIO project had existing health IT/health information exchange efforts when they joined the CORHIO initiative. Existing health IT adoption initiatives among major community and statewide health systems included the following:

- Kaiser Permanente (Denver and front range metro areas)
- Denver Health (Denver metro area)
- Children’s Hospital (Denver metro area)
- University of Colorado Hospital (Denver metro area)
- VA Hospital (Denver metro area)
- Centura Health System (statewide)
- Memorial Hospital (Colorado Springs)
- St. Mary’s Hospital (Grand Junction)
- Community Hospital (Grand Junction)
- Avista Adventist Hospital (Boulder/Longmont)

Emerging health information exchange initiatives, in addition to the AHRQ COHIE project, included the following:

- Quality Health Network (community HIE, western Colorado)
- Integrated Physician Network/Avista (community HIE among physicians, hospitals, and community health clinics, Boulder)
- HealthTrack (community HIE, Colorado Springs)
- Northern Colorado Health Alliance (community HIE among community clinics, hospitals, and mental health care providers, northeast Colorado)
- Rose Medical Group/Collaborative Care Network (physician independent practice association [IPA] groups)
- Rural Health Network
- Colorado Immunization Information System
- Colorado EKG Repository (CO EKG)

### *Current Health IT/HIE Landscape*

During 2006 and 2007, the Privacy and Security Solutions project was instrumental in supporting Colorado’s health information exchange implementation phase. CHI continues to support CORHIO, which was formally incorporated early in 2007, and much of the impact on the project has been made through CORHIO. CORHIO implementation activities focused in 2 areas. One priority is to establish a board of directors as well as organizational policies and practices, thereby ensuring a foundation for leadership, stakeholder participation and decision making, and technical operations. The second priority is technical implementation and the launch of live data exchange among its 4 AHRQ project partners by spring 2008.

Colorado health information exchange leaders view the Colorado health IT/health information exchange privacy and security environment in the context of the nationwide, overarching framework and desire a connection to this nationwide perspective to frame its

own work. The CORHIO framework is built on the input provided by those organizations that are expected to implement it, but relatively little information has been available from other states to help guide them in the process. A substantial amount of work has gone into this project, and although the leadership believes it will attain the goal of health information exchange between entities in 2008, concern remains about depleting the available resources within the state. Issues of sustainability appear to be the next challenge on the horizon.

### *Current Privacy and Security Landscape*

Both within and outside Colorado, the Privacy and Security Solutions project expanded the level of engagement of stakeholders and sources of expertise that are key to the successful implementation of Colorado's federated HIE infrastructure. Institutional security officers, privacy managers, and health information management professionals became involved in CORHIO policy development. National-level projects and staff (eg, the American Health Information Management Association [AHIMA] and RTI) brought important and timely information and perspectives to inform the CORHIO board and lend credibility among stakeholders, especially policy leaders, regarding Colorado's efforts toward privacy and security for health information exchange.

CORHIO's structure and operational roles, obligations, definitions, and accountabilities were defined through Colorado's Privacy and Security Solutions project work. Cataloging privacy and security issues on the project allowed the Colorado team to accelerate the process of policy building. The Privacy and Security Solutions project process enabled CORHIO to define the components of a secure technical architecture and develop a core set of privacy policies and practices that can be expanded for the state of Colorado. Participation in the Privacy and Security Solutions project brought about a careful and thoughtful consideration of privacy and security issues, on the basis of knowledge gained through collaboration, rather than haphazardly. The result has been the creation of an infrastructure for privacy and security and a body of key stakeholders with shared knowledge.

The Policy and Compliance Committee of CORHIO is charged with developing privacy and security policies and defining enforcement methods and remedies. Formal state-level priorities for CORHIO include authentication, role-based access, policies for specially protected information, consistent methods for obtaining and tracking patient authorization, and auditing.

To date, the Colorado Privacy and Security Solutions project has

- prepared an analysis of the legal and regulatory framework for privacy and security in the state and submitted it to RTI in April 2007;
- convened working groups to address privacy and security issues for CORHIO ranging from initial broad-based meetings to subsequent policy-writing meetings;

- had broader stakeholder meetings for all interested parties in the state, including statewide provider organizations, consumer organizations, other data sharing organizations, and technical groups;
- initiated the formation of a Consumer Advisory Committee, with the help of the Colorado Consumer Health Initiative (CCHI), to focus, in part, on communication about privacy and security issues; and
- endorsed both policies and data sharing agreements that will further the Point of Care data exchange model being launched in Colorado in early 2008.

The Privacy and Security Solutions project, through CORHIO, has supported statewide understanding of Colorado's privacy and security environment; the development of a diverse and active CORHIO board of directors; helped the CORHIO board refine its governance structure; enabled outreach to a wide variety of stakeholders; and assisted in the development of policies and agreements that will allow Colorado's Point of Care model to proceed forward as a communitywide effort and a foundation for CORHIO's future success as a statewide RHIO.

CORHIO's corporate structure and governance model have been based on the work of the Privacy and Security Solutions project. A diverse group of stakeholders have reached consensus on a set of statewide benefits that can accrue from health information exchange by engaging in candid discussions about the future of CORHIO and the federated model on which it has been built.

Similarly, the CORHIO-adopted privacy policies and data sharing agreements have been facilitated through the Privacy and Security Solutions project. Common ground for these efforts developed because there was a forum in which to discuss perspectives, educate stakeholders, and craft practical solutions to common issues that will affect future health information exchange activities. The Privacy and Security Solutions project offered CORHIO much-needed support in funding, technical and management direction and tools from the RTI project staff, advice from the Technical Advisory Panel, and collaboration with teams in other states. These resources enabled the Colorado team to engage successfully in these endeavors.

#### **4.1.6 Connecticut**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Connecticut's proposal for the Privacy and Security Solutions project depicted the state's privacy and security concerns and challenges surrounding health IT and health information exchange. The Connecticut state project team reported that barriers and solutions would have to be addressed on multiple fronts to advance the electronic sharing of health information statewide, including legislative, legal, financial, administrative, clinical,

technical, and motivational issues. Numerous health IT/health information exchange initiatives existed in Connecticut when the proposal was written, including the following:

- The Connecticut Health Alert Network, a computer-based system, linked local health departments to one another and to other organizations critical for preparedness and response in case of an emergency.
- The Connecticut Electronic Disease Surveillance System provided a web-based disease surveillance application, allowing for electronic capture of disease data, case assignment and tracking, addition of public health case investigation data, and data export.
- The Newborn Screening System was a database and data-gathering application for hospitals.
- The Electronic Cancer Pathology Reporting System provided for automated transmission of mandated reporting by Connecticut pathology laboratories directly to the Connecticut Cancer Registry System.
- The Connecticut Tumor Registry System collected and processed all reported cancer information, including cancer diagnosis, follow-up, treatment, and survival data from all health care providers since 1935.
- The Connecticut Immunization Registry and Tracking System was designed to provide a real-time interface for the repository of all childhood immunization events for children in the state.
- The Medicaid Management Information System (MMIS) processed millions of claims from more than 6000 providers and vendors enrolled in the Department of Social Services' health care programs.
- The US Department of Veterans Affairs' computer-based patient care system tracked all of the agencies' clients and tracks the health care they receive across systems.
- The Connecticut Department of Insurance System provided an online interface for reporting medical malpractice claims.
- The Connecticut Substance Abuse Data Sharing project involved 10 state agencies that share administrative data.
- The Behavioral Health Information System (BHIS) replacement system replaced the current BHIS as a state-of-the-art information system to facilitate clinical decision making, service planning, documentation, outcomes measurement, and analysis of service-system performance.
- The Quality Review Initiative was designed to provide the Department of Developmental Services with an overall quality review indicator, using electronic document work flow and a web-based interface for private providers.
- The Governor's Interim Geospatial Information Council began coordinating and promoting technology and the sharing of geospatial information among key executive branch state agencies, essential to providing a coordinated, swift, and effective response in an emergency.
- eHealth Connecticut focused on developing a statewide HIE. In January 2006, official Articles of Incorporation were filed to make eHealth Connecticut a 501(c)(3) corporation.

- The Connecticut Health Information Management and Exchange (CHIME) Program was developed to link inpatient, ambulatory surgery, and emergency department clinical abstracts for all Connecticut hospitals in a longitudinal data warehouse.
- Qualidigm, Connecticut's Quality Improvement Organization, was awarded a contract with the CMS DOQ-IT project to provide free assistance for primary care physicians and their office practices to help them make informed decisions in selecting, implementing, and effectively using EHR systems.
- Community-based initiatives organized around a hospital or medical practice were implemented, including The Waterbury Health Access Program, Yale's Electronic Records to Improve Care for Children with Asthma, the Middlesex Area Physician Group Practice demonstration project, and The Eastern Connecticut Health Network, Inc.

### *Current Health IT/HIE Landscape*

The initiatives listed above are all part of the current landscape of health IT and health information exchange in Connecticut. The Connecticut project has reported an important change in the way these individual initiatives now relate to one another. Working on project goals related to privacy and security issues helped these stakeholders to recognize the importance of learning from one another on other issues related to health IT and health information exchange, and the Privacy and Security Solutions project was a major factor in building and sustaining collaborations. Stakeholders from these organizations and initiatives regularly interact in open forums to discuss issues with hospitals, private agencies, and other state agencies and frequently participate in work groups on a wide variety of topics.

Several additional outcomes of the Privacy and Security Solutions project for Connecticut relate to health IT and health information exchange in general. The project led to the articulation of work overdue at the state level, bringing issues and direction to the forefront. The project team established a baseline of the state's activity, which has been reviewed by state officials and is being supported by them (eg, through requests for proposals) for future work on health information exchange. The Connecticut team was encouraged to participate in multistate projects.

Finally, the project was about to connect with new activities such as:

- Yale New Haven Hospital and the Hospital of St. Raphael established a local RHIO-like exchange of emergency department information.
- Hartford Hospital PHO, St. Francis Hospital PHO, The Hospital of Central Connecticut, Grove Hill Medical Center, and Qualidigm joined together as the Greater Hartford Coalition for Quality Healthcare to develop a project involving health information exchange (RHIO activity).
- The Department of Social Services received a Medicaid Transformation Grant to implement e-prescribing and a medication history for Medicaid patients.

### *Current Privacy and Security Landscape*

Although multiple health IT and health information exchange projects were occurring in Connecticut before the Privacy and Security Solutions project, there were no state mandates, general funding, or agreed-upon business plans to build a comprehensive HIE in Connecticut and no specific focus on privacy and security of health information exchange. Without a uniform strategy on privacy and security, state agencies, hospitals, and other entities experienced obstacles in creating collaborations and in the technical development of health IT systems that could communicate with each other.

Following the Privacy and Security Solutions project methodology, the team identified an array of challenges to appropriate and secure health information exchange. In addition, the team noted that many stakeholders were unaware of other health IT/health information exchange initiatives occurring in the state. The initial barriers to health information exchange included issues of patient consent, minimum disclosure requirements, the logistics of a RHIO, the sharing of radiology images, and other technical issues. To address these barriers, the team identified a range of solutions documented in their Analysis of Solutions Report.

In the initial phases of the project, the Connecticut team offered a venue for collaboration among stakeholders about privacy and security practices and policies. The team found that although stakeholders were often working towards similar goals, their work was unconnected (“siloed”). Stakeholders were frequently unaware of one another’s activities and of the number of instances where information exchange might be required. To link stakeholders together, the Connecticut team held open forums to discuss issues with hospitals, private agencies, and other state agencies, and invited a wide range of individuals, including providers, to participate in work groups. In November 2006, the team held a privacy and security workshop. The information gleaned from this workshop, such as the lack of knowledge across stakeholder groups, enabled the team to work proactively in subsequent stages of the project. The project fostered a common understanding of privacy and security policies and focused procedures across multiple stakeholder groups.

This recognition of the importance of health IT and health information exchange led to the July 13, 2007, authorization of the Department of Public Health and the Office of Health Care Access to develop a request for proposals to designate a RHIO to coordinate Connecticut’s HIEs. Public Act No. 07-2: An Act Implementing the Provisions of the Budget Concerning Human Services and Public Health mandates the Connecticut Department of Public Health, in conjunction with the Office of Health Care Access, to develop a statewide health IT plan. This plan will include (1) general standards and protocols for health information exchange; (2) electronic data standards to facilitate the development of a statewide integrated electronic health information system for use by health care providers and institutions by funded by the state including standards on (a) security, privacy, data

content, structures and formats, vocabulary, and tradition protocols; (b) for compatibility for any national data standards in order to allow for interstate interoperability; (c) for permitting the collection of health information in a standard electronic format; and, (d) for compatibility with the requirements for an electronic health information system; and (3) pilot programs for health information exchange and projected costs and sources of funding. This work is being done in a competitive bid process in which the entity awarded this contract must be designated as the lead health information exchange organization for the state during the time period of December 1, 2007–June 30, 2009.

The Connecticut team has been successful in participating in and supporting privacy and security work at the local, state, interstate, and national levels. Common policies and procedures have enabled the creation of a local RHIO-like exchange of emergency department information between Yale New Haven Hospital, and the Hospital of St. Raphael. Hartford Hospital PHO, St. Francis Hospital PHO, The Hospital of Central Connecticut, Grove Hill Medical Center, and Qualidigm have formed a partnership to work towards health information exchange.

Connecticut has also worked across states and with national organizations. The team has begun dialogues with teams in Massachusetts and New Jersey to explore the need for interstate information exchange, and explore the privacy and security implications of doing so. At the national level, the team has also strengthened their relationship with the National Governors Association (NGA) and enhanced their participation in several multistate projects, including the Health Information and Management Systems Society/General Services Administration (HIMSS/GSA) project and the Liberty Alliance.

In working through the analysis of solutions, Connecticut's work groups identified common building blocks to achieve health information exchange in identification, authentication, authorization, access control, and audit. As examples of building blocks, practical solutions need to be found for: (1) recognition of person (patient and provider); (2) cross-indexing; (3) record locator services; and (4) common exchange protocols. Identifying these building blocks enabled the team to recognize the need for common protocols and processes. The team is working to integrate smaller efforts into a macro-level system change that will develop and deploy common standards and processes.

The Connecticut team chose one key project for their 6-month implementation period: defining the provisions for digital identities for the health care workforce and creating a final report of those provisions. The team selected this project because it was seen as one of the foundational components of successful health information exchange and because it could be accomplished within the 6-month window.

The primary objective of this project was to define the specifications for trusted digital identities for authentication, authorization, access control, and data integrity for digital signature purposes. The project identified specific system requirements for identity

management systems that correspond with the state Department of Public Health's practitioner licensure process. In addition, the team identified national standards to provide a guideline for the authorization of practitioners and health care institutions. The final specifications will be specific to Connecticut, although they will be written so that other states can easily replicate Connecticut's process. When fully implemented, the project will support secure health information exchange by enabling trusted remote identification and authorization, and usage of digital signatures (including those for all tiers of prescriptions).

Connecticut continues to leverage the work done in the early stages of the project in working toward secure electronic health information exchange. They will continue this work in 2008 as a member of a multistate collaborative examining the implementation of standards.

The Privacy and Security Solutions project increased the level of public-private collaboration in Connecticut. State agencies have held open forums with hospitals, private agencies, and other state organizations. The Privacy and Security Solutions project has engaged the state's Department of Consumer Protection in discussions of privacy and security to assist in developing greater awareness among patients and their families. Educational forums have enabled Connecticut to share information with providers and consumers, stimulating discussions among a broad array of participants. The project has also encouraged and facilitated regional interactions and collaborations with other states about interstate health information exchange and their own RHIO initiatives.

#### **4.1.7 Florida**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In May 2004, Governor Jeb Bush called for the creation and promotion of a plan for the development and implementation of a Florida health information infrastructure (HII). He established the Governor's Health Information Infrastructure Advisory Board, which was charged with 4 tasks to be completed by June 30, 2007. These tasks included (1) advising and supporting the Agency for Health Care Authority (AHCA) as it develops a strategy for the adoption and use of EHRs, (2) identifying obstacles to the implementation of an effective HII in the state and providing AHCA with policy recommendations to remove or minimize these obstacles, (3) advising the executive and legislative branches on issues related to the development and implementation of the HII, and (4) assisting AHCA in ensuring that the strategy and plan preserve the privacy and security of health information as required by law.

Between the time of the board's creation and the writing of the Privacy and Security Solutions project proposal, the board and AHCA made substantial progress in the promotion of electronic health information exchange. Activities included the following:

- AHCA and the board hosted several conferences and workshops to gather information and advice from national experts, as well as Florida stakeholders, about health information infrastructures.
- The board conducted extensive outreach activities to encourage local health information network initiatives across the state.
- AHCA and the board implemented the Florida Health Information Network (FHIN) grants program in January 2006. The first grants cycle funded 5 health information exchange planning grants, 3 health information exchange operations and evaluation grants, and 3 practitioner training and technical assistance grants to encourage the adoption of EMRs.
- AHCA and the board produced the first draft of a white paper describing architectural considerations for a state HII for public comment.

### *Current Health IT/HIE Landscape*

The health IT/health information exchange landscape in Florida continues to develop. Today, the state HIE initiative is led by the Florida Center for Health Information and Policy Analysis. The FHIN is made up of RHIOs within Florida, and the Florida Association of RHIOs is an emerging force. AHCA collaborates with other national health IT/HIE initiatives, such as the State e-Health Alliance and the State-Level HIE Consensus project. The Florida state team has an open and collaborative working relationship with the state HIEs and has encouraged their participation. The most recent health information exchange initiative in the state is the electronic prescribing clearinghouse, which provides information on electronic prescribing products available in Florida on the agency's website ([www.fhin.net](http://www.fhin.net)). The agency is also developing a plan for the integration of Medicaid EHRs within RHIOs, which will be first offered to FHIN grantees in 2008. Florida now has 8 operational health information exchanges that have been funded, in part, by the FHIN grants program.

A report by the US Department of Health and Human Services' Office of Inspector General found that Florida is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Iowa, Kansas, Louisiana, Mississippi, Vermont, Wisconsin, and Wyoming.)

### *Current Privacy and Security Landscape*

Florida, like many other states, has struggled in balancing the concerns for privacy and security with the potential benefits of electronic health information exchange as a solution to the inefficiencies and patient safety issues that exists in the health care system. Prior to engaging in the Privacy and Security Solutions project, Florida had not hosted any activities specifically related to examining privacy and security issues in health information exchange.

The community was quite aware of the issues and concerns about building and maintaining a private and secure health information exchange, as well as the barriers to the adoption and utilization of electronic health records among health care providers, but was unaware of the actual drivers behind the reluctance to share health information. The Privacy and Security Solutions project allowed Florida to bring together numerous stakeholders to discuss the problems associated with health information exchange and to devise potential solutions.

As a result of the work conducted under the Privacy and Security Solutions project, the stakeholder work groups discovered that many of the problems related to health information exchange resulted from variations in how privacy and security policies are applied to actual business practices in the health care industry. The variation in privacy and security practices and policies itself resulted in unnecessary barriers to health information exchange. The inconsistency in state and federal laws, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice were significant barriers to health information exchange.

An early milestone of the Privacy and Security Solutions project was the first LWG meeting held in August 2006. As a result of interest and support of participants, AHCA proposed to reconvene the project's LWG as part of its implementation proposal. With the additional funding Florida received for the implementation period, the LWG was reconvened to assist in the completion of an analysis of Florida laws related to health information exchange begun in the project's first year. The LWG was tasked with the development of recommendations for the reform and potential consolidation of privacy and security-related statutes and laws. The LWG completed this task and created the report, *Analysis of Florida Statutes Related to Health Information Exchange*. They recommended that certain inconsistencies in Florida law be addressed but did not address the consolidation of statutes.

The Florida Privacy and Security Solutions team also created and implemented a risk self-assessment tool in collaboration with Florida RHIOs. The risk self-assessment tool was developed to be easy to use, with useful features for tabulating the results of the self-assessment test. Although the tool currently addresses only security issues, the design of the tool allows for the addition of modules that address privacy policies and state laws.

AHCA views the risk self-assessment as an educational tool to increase awareness of new entrants and nontechnical stakeholders. AHCA plans to develop a website where the latest information on privacy and security standards and the tool will be posted. This information gathering process will also assist AHCA as it begins to work with RHIOs to develop uniform privacy and security policies for the FHIN.

The Florida team reported that one tangible outcome of the Privacy and Security Solutions project in Florida has been the growth and development of a community of stakeholders that recognize the importance of privacy and security and communicate openly with each

other. The project was successful in raising awareness of the need to reform state laws related to the privacy and security of health information exchange, the need for clear and concise legal standards for health information exchange, the need for uniform privacy and security policies across RHIOs, and the need for more effective provider and consumer education.

Initially, there was very little communication among the various RHIOs in Florida other than formal presentations at Governor's Advisory Board meetings. Through the Privacy and Security Solutions project, representatives from the RHIOs began meeting with each other at Privacy and Security Solutions project meetings. This collaboration fostered the Florida Association of RHIOs, which is helping to integrate the various health information exchange projects in the state. More recently, the RHIO-hosted community forums have provided an opportunity for AHCA and RHIO representatives to discuss the privacy and security issues and highlighted the opportunity for AHCA to facilitate the exchange of best practices among RHIOs. As a result, AHCA has proposed adding provisions regarding the transparency of privacy and security policies to the requirements of the FHIN Grants Program.

One unanticipated and positive outcome of the Privacy and Security Solutions project in Florida is that it has established and reinforced the role of state government in providing leadership to ensure the privacy and security of health information exchange. The Privacy and Security Solutions project has provided an alternative venue for interaction among AHCA, RHIOs, and other stakeholders through participation in the project. It has also encouraged the continued focus on the development of uniform privacy and security policies that facilitate health information exchange.

The Governor's Health Information Infrastructure Advisory Board was disbanded in June 2007, as originally planned. Although no formal governance structure for privacy and security took its place, AHCA has the authority to establish regulations related to the FHIN. AHCA and the FHIN are carrying forward many of the board's goals. The FHIN, as a statewide collaboration of RHIOs and AHCA, focuses on privacy and security issues that are fundamental to the creation of an integrated statewide network. AHCA has developed a high-level privacy and security policy document, the *Privacy and Security Fact Sheet*, as a first step in establishing statewide standards for RHIOs. The FHIN public-private partnership recognizes that privacy and security considerations are foundational for the interoperability of health information.

Participation in the Privacy and Security Solutions implementation project has allowed Florida to begin to address numerous objectives related to the goals established for this project. The experience gained through this project has reinforced the need for leadership and coordination to make best use of available resources.

#### **4.1.8 Illinois**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In 2005, the Illinois General Assembly passed and Governor Blagojevich signed legislation (Public Act 94-646) creating the Electronic Health Records (EHR) Taskforce. The primary objective of the task force was to create a plan for the development and use of EHRs in the state to improve the quality of patient care, increase the efficiency of health care practice, improve safety, and reduce health care errors. The task force held more than 40 meetings and issued its report on December 27, 2006. It recommended the creation of a state-level HIE under the governance of a not-for-profit organization called the Illinois Health Information Network (ILHIN). ILHIN would also work with the Illinois Department of Public Health on a program to foster the adoption of EHRs by health care providers.

Besides the EHR Taskforce, Illinois had several ongoing health IT/health information exchange initiatives. The Illinois Department of Public Health developed a system to provide integrated data sharing and support for multiple health and human service programs. This system was transferred to the Illinois Department of Human Services when that agency was created. Another initiative, the Illinois Health Network, offered the infrastructure to enable hospitals and health care professionals to participate in health information exchange, and the Illinois Hospital Research and Educational Foundation was awarded \$1.5 million from the state to begin implementation of the network. Additionally, many hospitals and health care systems in the state have initiated or purchased EHR systems for their facilities.

In the early 1990s, a group known as the Chicago Health Information Network attempted to develop an HIE. Because of lack of governance and funding, however, the group disbanded. Although there has been no success in establishing a RHIO, an organization known as the Northern Illinois Physicians for Connectivity (NIPFC) is working to fulfill the goals of a RHIO. NIPFC encourages and facilitates the use of health care technology among its members by maximizing economies of scale. Its vision is to ensure the privacy and security of confidential information yet allow health information to be shared by way of a patient index.

##### *Current Health IT/HIE Landscape*

Governor Blagojevich issued an executive order on July 13, 2006, that created the Division of Patient Safety within the Illinois Department of Public Health. The new division is to consolidate the state's efforts for dealing with medical errors and focus on improving patient safety. The governor gave this new division an important electronic health information role as part of its patient safety mandate with respect to prescription drug safety. Among other provisions, the governor charged it with the following responsibilities:

- Encourage all medical providers to use e-prescribing programs by 2011. E-prescribing allows a physician to legibly write and electronically send prescriptions to reduce the risk of medication errors.

- Evaluate the areas in Illinois that need enhanced technology to support e-prescribing programs.
- Determine the types of technology needed to implement the e-prescribing program.

The health IT/health information exchange landscape in Illinois has been challenging, largely because of state budget constraints. The status of the Illinois Health Network is in doubt because no additional funding has been appropriated.

Legislation to implement the recommendations of the EHR Taskforce, House Bill 1254, was approved by the Illinois General Assembly during the spring 2007 session. However, Governor Blagojevich vetoed an amendment to change the ILHIN from a not-for-profit organization to an advisory body and to shift responsibility for implementing the state-level HIE to the Illinois Department of Healthcare and Family Services (the state Medicaid agency). The House of Representatives did not react to veto, and the bill has died.

Nonetheless, efforts to establish interoperable systems persist in the state. A number of hospitals are trying to initiate EHRs and link to associated physicians. Specific plans to link the systems together are still under development. The Community Health Record of Illinois is encouraging the use of personal health records and working with interested persons on the creation of a white paper on the subject. Most Illinois hospitals are part of an integrated delivery system, and they are beginning to adopt and accept e-prescribing.

The Privacy and Security Solutions project has facilitated collaboration with an expanded level of stakeholders, such as AHIMA and individual providers. This collaboration has been helpful to the state.

Current Illinois initiatives are as follows:

- Illinois Health Network
- Northern Illinois Physicians for Connectivity (with the goal of encouraging and facilitating use of health IT among members and working toward private and secure transmission of information)
- Evanston Northwestern Health EHR
- AHRQ grant (\$1.5 million) for ambulatory EHRs
- Illinois Hospital Association RHIO committee on policy making
- Blue Cross/Blue Shield (building on claims-based architecture)
- Illinois Foundation for Quality Health Care (DOQ-IT)
- Public Health (Illinois-National Disease Surveillance System, PHIN integration)

The new Division of Patient Safety in the Department of Public Health is collaborating with the following states on health IT/health information exchange issues and ideas:

- Massachusetts eHealth Collaborative

- Indiana Health Information Exchange
- Utah Health Information Network
- Tennessee’s Volunteer eHealth
- Minnesota e-Health Initiative

There are several examples of health IT in practice. The Alliance of Chicago Community Health Services links 4 community health centers serving over 79000 patients at 25 sites. Their activities include implementing their EHRs in a network of community health centers, developing a data warehouse for clinical and system quality improvement, and using the EHRs/data warehouse for evidence-based practice measures. The Katherine Shaw Bethea Hospital in Dixon, Illinois, is currently providing controlled, secure physician access to internal applications (eg, using electronic signatures) and enabling patient information to be shared between emergency departments, local mental health agencies, and public health agencies. The Illinois Department of Public Health is currently developing a system to improve the collection of laboratory results data from participating hospitals in the state.

#### *Current Privacy and Security Landscape*

Participation in the Privacy and Security Solutions project has led to increased interactions with organizations and individual providers at a detailed level that Illinois had not previously experienced. The project team in Illinois has played an important role in addressing privacy and security issues relating to health information exchange. The legislatively mandated health information exchange study group, the EHR Taskforce, deferred to Illinois project team on privacy and security issues. The task force and the Privacy and Security Solutions team in Illinois also shared a core group of members to maintain a link between the efforts of the 2 entities. While the EHR Taskforce was laying out a blueprint for the development of a state-level HIE, the Privacy and Security Solutions team identified privacy and security challenges facing that effort.

Although the enabling legislation that would have created the ILHIN was not approved, state policy makers continue to pursue the creation of a state-level HIE and initiatives to foster the widespread adoption of EHRs and local health information exchanges. The implementation priority for the Illinois team was work with governmental and private sector stakeholders—a public-private partnership—to move forward on privacy and security issues that need to be addressed by the governance structure of a state-level HIE. The Illinois project proposed to accomplish this task by establishing 2 work groups, each focusing on a distinct privacy and security-related product.

A Privacy and Security Work Group was formed to develop draft privacy and security policies and recommendations for consideration by the governance structure of a state-level HIE. The work group developed a draft document, “Recommendations on Privacy and Security Policies,” that focused on the following 12 privacy and security areas:

- privacy and security philosophy,
- patient rights with respect to information privacy and security,
- protection of caregiver information,
- privileges and obligations of researchers,
- retention and destruction,
- information privacy and security program,
- accountability and responsibilities,
- access to information,
- records of access,
- disaster recovery/business resumption plans,
- information privacy and security awareness training, and,
- remedies.

An LWG was convened to draft a uniform model patient EHR/health information exchange consent form for possible use by the state-level HIE, clinicians, health care facilities, and other providers. During its deliberations, the LWG developed 3 forms after they determined that one form would not address the different issues faced by providers and an HIE under state and federal law. The 3 forms are the:

- Notices of Privacy Practices Insert
- Consent for Use and Disclosure of Certain Types/Categories Protected Health Information
- Authorization for Use and Disclosure of Protected Health Information for Research

The products of the 2 work groups were sent to interested stakeholders for review and comment on October 23, 2007. Comments were to be returned by November 7, 2007. Both work groups have met to discuss the comments that were received and made revisions to address many of the comments.

During December, these products will be finalized by the work groups and then be reviewed and approved by the project's steering committee. The "Recommendations on Privacy and Security Policies" document will be shared with the Illinois Health Information Exchange Advisory Committee, a committee that has been formed by the Departments of Healthcare and Family Services and Public Health to continue the implementation planning for the development of a state-level HIE. The LWG forms will be distributed to health care providers who will be encouraged to use the model forms or incorporate text from them into their existing forms.

The impact of the Privacy and Security Solutions project in Illinois is that the state is better prepared to deal with health information exchange privacy and security issues. Because of

the project, stakeholders have become more engaged in addressing privacy and security issues. The project has also brought a broad spectrum of stakeholders together to address barriers to health information exchange in Illinois. The project has been instrumental in sharing the lessons learned by other states.

#### **4.1.9 Indiana**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Indiana has been a leader in health information exchange, health data standards, research, and quality improvements in patient care in both the private and public arenas for decades. Indiana has collaborated with the state government, the federal government, private research institutes, and various medical institutions to further the development of health information exchange in Indiana.

Regenstrief Institute is a medical research institute affiliated with Indiana University. The Regenstrief Medical Record System (RMRS), created in 1972, is one of the nation's first EMR systems and serves as the day-to-day EHR system for several area hospital systems and community clinics. In 1995, Regenstrief used the RMRS structure to create the Indiana Network for Patient Care (INPC), the nation's first citywide HIE. INPC began as a long-term partnership among the 5 major Indianapolis hospital systems and 1 large primary care group. The primary purpose of the INPC is to provide clinical information at the point of care for the treatment of patients. At the time of the first Privacy and Security Solutions project proposal, all 5 of the major Indianapolis hospital systems (a total of 14 hospitals) sent most of their clinical content to the INPC. Other hospitals and physician practices have also become INPC participants or have agreed to contribute data for INPC purposes. Regenstrief has been involved in several federal contracts, the Nationwide Health Information Network (NHIN) prototype project funded by the Office of the National Coordinator for Health Information Technology (ONC), and the state-Level HIE consensus project.

The Indiana Health Information Exchange (IHIE) is a nonprofit corporation formed in 2004 through a collaboration of health care institutions with a vision to "wire" health care—first in central Indiana and eventually across the entire state—by capitalizing and expanding on Regenstrief's INPC infrastructure and software tools. The first service offered by IHIE was Regenstrief's implementation of DOCS4DOCS<sup>®</sup> (a tool created to provide clinical messaging functions for local area physicians), which involved hospitals' and labs' paying a fee for the DOCS4DOCS system to deliver test results to physicians. At the time of the first Privacy and Security Solutions project proposal, 2900 out of 3200 physicians in central Indiana were on the system.

The Indiana State Department of Health (ISDH) is working with Regenstrief on the Public Health Electronic Surveillance System (PHESS), a project to establish a statewide public

health surveillance network that links all 114 hospitals in the state by 2008, allowing them to share emergency department encounter data. As of March 2006, 50 hospitals were enrolled in PHESS. ISDH uses data collected by PHESS for public health purposes, such as outbreak detection and bioterrorism surveillance.

Local HIE initiatives in Indiana, but outside Indianapolis, include the Michigan Health Information Network near the state border in the South Bend/Elkhart region, efforts in Fort Wayne and Evansville, and the e-health collaborative in Bloomington.

### *Current Health IT/HIE Landscape*

Indiana's strategy toward health IT/HIE development has been to capitalize on and support existing health information exchange efforts in the state. Consequently, the environment is collaborative, growing, and able to replicate.

Since the initial Privacy and Security Solutions project proposal, many of the existing health information exchange efforts have grown. The INPC has increased in geographic scope to encompass surrounding counties, has grown from 14 to 21 hospitals, and has added payer claims data for Indiana (including Anthem and Indiana Medicaid). The demand for INPC membership is expanding rapidly.

IHIE continues to expand its customer base for Regenstrief's DOCS4DOCS clinical messaging system, now serving more than 5000 physicians in central Indiana. It delivers more than 1 million messages per month through the system, saving millions of dollars per year by eliminating duplicate tests and administrative costs. IHIE's focus is on providing the service in other regions of the state.

Regenstrief and IHIE are collaborating on providing quality performance measurement reports for participating payers and providers, supported by funding from federal and private sources. Regenstrief Institute, with participation from IHIE will continue its groundbreaking work in health information exchange by beginning the trial implementation of the NHIN model, funded by a \$2.5 million contract from the US Department of Health and Human Services to Indiana University.

Regenstrief continues to work with ISDH on advancing public health initiatives through health information exchange and analysis. The PHESS system continues to expand and now connects ISDH with more than 76 hospital emergency departments in Indiana.

### *Current Privacy and Security Landscape*

In the assessment of variations in business practices and policies, conducted early in the Privacy and Security Solutions project, the Indiana project team concluded that there were few legal barriers to health information exchange in Indiana.

However, the team did find challenges with respect to federal law. One specific issue concerned health care facilities that offered substance abuse treatment (covered under 42 C.F.R. pt. 2), and other forms of medical care (“mixed use facilities”). There were at least 2 such facilities that wished to join the INPC. Concerns about complying with federal law limited the sharing of any of the data from those facilities with the INPC. Although there were other federal issues of concern, the Indiana team selected the 42 C.F.R. pt. 2 challenges to address first.

The Indiana team identified and reviewed the main issues regarding 42 C.F.R. pt. 2 drug and alcohol abuse treatment information facing electronic health information exchange efforts. Additionally, Indiana is leading a multistate committee comprised of 17 states to explore how 42 C.F.R. pt. 2 intersects with electronic health information exchange by working closely with the Substance Abuse and Mental Health Services Administration (SAMHSA) to clarify interpretation of the regulations and by vetting some different models for electronically implementing the data exchange process.

The Indiana team, along with representatives from Minnesota, Michigan, and North Carolina, met with SAMHSA, ONC, and Legal Action Center on November 14, 2007, to discuss the scenarios document produced by the Indiana team, as well as next steps. The Department of Health and Human Services (HHS) representatives commented that the document was very thorough and useful. At the meeting, much progress was made in the resolution of certain issues, and some other issues were taken under advisement (and required further research by HHS). Federal guidance from HHS on this issue will aid HIEs and help clear up ambiguities in interpretation of this law.

Throughout the course of the Privacy and Security Solutions project, Indiana has been able to increase the understanding of privacy and security issues in the state by engaging a broad array of stakeholders from both public entities and private industry in discussions on health information exchange. Additionally, collaborative efforts with Michigan, Ohio, and Kentucky have enabled Indiana to make tangible progress toward interstate exchange in the Midwest.

Funding, project resources (including assessment toolkits and the Technical Advisory Panel) and the opportunity to collaborate with similarly focused teams in other states have provided a base from which new interstate relationships have developed, as well as a more direct dialogue with ONC and SAMHSA. The Indiana team believes this has helped move the country forward in identifying privacy issues and highlighted the need for more work to be done in resolving interstate data sharing issues. While states may be at different stages in their development of health information exchange, a new level of understanding and awareness of privacy issues and potential solutions has been achieved. States have become more well versed in what other states are doing to overcome barriers, and they have been

able to learn from others' mistakes and take advantage of solutions that might also work in their own state.

#### **4.1.10 Iowa**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

The Iowa HIT Initiative was formed in November 2004 to promote accelerated adoption of health IT to improve quality, safety, and value in Iowa's health care environment. This collaborative partnership, led by the Iowa Foundation for Medical Care and the Iowa Medical Society, includes more than 90 individuals representing more than 30 Iowa health care organizations. The Iowa HIT Initiative is a voluntary effort that focuses on engaging and motivating Iowa providers to implement health IT. The group is guided by a 16-member steering committee comprising physician leaders and professional organizations across Iowa. The steering committee formed a health information exchange subcommittee, and a call for volunteers had been issued at the time the proposal was written.

In the spring of 2005, Iowa lawmakers approved legislation expanding Medicaid services to previously uninsured adults between the ages of 19 and 64 and living below 200% of the federal poverty level. The Iowa Cares Act includes money to support the use of health IT by Medicaid providers. Additionally, the Department of Human Services received a grant to begin development of interoperability standards and data exchange protocols for Medicaid providers.

In November 2005, the University of Iowa's Center for Health Policy and Research received funding to conduct a literature review on the effectiveness of EHRs. The white paper provided an overview of the national and local environment as it relates to health IT, barriers and benefits of technology adoption, the value of interoperability, and recommendations for state actions.

The Iowa Health Information Management Association publishes the *Iowa Guide to Medical Record Laws*, which serves as a resource for professionals handling health information. Sources used in creating this compilation include the statutes, regulations, and common law of the United States and Iowa, current hospital practices, statements of associations and organizations, and expert opinion.

In September 2004, AHRQ awarded 3 contracts to researchers in Iowa as part of an overall effort to fund and promote the use of health IT through the development of networks for sharing clinical data and to fund projects for planning, implementing, and demonstrating the value of health IT.

### *Current Health IT/HIE Landscape*

The Iowa HIT Initiative, led by the Iowa Foundation for Medical Care and the Iowa Medical Society, is a statewide effort to advance the use of health IT to improve quality, safety, and value of health care in Iowa. The initiative recently completed a survey dedicated to tracking health IT adoption in Iowa physician offices, with emphasis on EHR rates. The survey report, *Health Information Technology Adoption in Physician Offices, a Summary of Survey Findings in Iowa* (Iowa HIT Initiative, 2007), shows that 25% of physician offices reported EHR adoption in 2007, compared with 18.3% in 2005. In addition, the Iowa Medicaid program has implemented an electronic records system that provides web-based access to patient-level claims data for providers statewide. This program became active in the spring of 2007.

The greatest impact of the Privacy and Security Solutions project has been the ability to engage all stakeholders in discussions about health information exchange and to bring privacy and security issues to the forefront. This level of awareness among payers, providers, and consumers had not been explicitly achieved. In fact, 2 years ago, when the Iowa HIT Initiative started, people discussed implementation of health IT but not the exchange of information. Previous health IT initiatives were inwardly focused to a large extent. This project brought forward the issue of secure exchange practices and how Iowa state laws affect that process. Iowa has begun to build sustainability by encouraging discussion and establishing panels of those who have agreed to continue work after the Privacy and Security Solutions project. For example, Iowa has chief information officers and clinicians who are highly motivated to stay involved because of their increased awareness. The resulting commitment to see work through to completion has been the project's greatest impact for Iowa. The state project team remains hopeful about identifying further implementation funding, and a person has been dedicated to researching funding opportunities.

A report by the US Department of Health and Human Services' Office of Inspector General found that Iowa is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Kansas, Louisiana, Mississippi, Vermont, Wisconsin, and Wyoming.)

### *Current Privacy and Security Landscape*

An important impact of the Privacy and Security Solutions project on the privacy and security landscape in Iowa has been a shift in perspective from a narrow view of health IT adoption—implementing intra-organizational systems—to both health IT adoption and

electronic health information exchange between organizations. Project participants in the legal community, consumers, and private entities such as universities and large health systems now recognize that progress is not simply a matter of adopting technologies for storing and retrieving health information within a single health care organization. There is now an outward focus on coordination among partner organizations in exchange rather than an inward focus on technology decisions. The project has also enabled Iowa to establish interstate relationships, particularly with Minnesota, Nebraska, North Dakota, and South Dakota, to address privacy and security issues that affect interstate exchange of health information.

The Privacy and Security Solutions project has fostered discussions with the Iowa EMR Task Force and member legislators about the next steps. Both groups have identified a need to establish a statewide governing body in Iowa to oversee e-health activities and provide a funnel for funding resources. The state project team is currently outlining the various options for consideration by the task force. Iowa is also conducting an implementation project by which 5 expert panels will produce a set of privacy and security recommendations to inform future health information exchange efforts in the state. The implementation effort includes a pilot health information exchange demonstration project to develop and endorse a continuity of care document. In combination with Iowa's guide to best practices for private and secure exchange, the continuity of care document will facilitate private and secure exchange of health information.

The project's legal panel updated Iowa HIPAA pre-emption analysis to take account of the conclusions of the Solutions Work Group. The legal panel has agreed to continue meeting quarterly as a legal resource to support additional activities of the Privacy and Security Solutions project. The group has prioritized actions: (1) to address safe harbors, and (2) to address data breach/liability law.

In addition, a project team working on patient consent issues completed a patient consent matrix to clarify Iowa and HIPAA consent requirements. The team shared this matrix with the multistate HISPC collaborative on patient consent. The team also evaluated 5 potential models for health information exchange in Iowa and compiled findings in an organized framework for comparison.

In consideration of interstate data exchange, the Iowa team agreed to pilot test data sharing agreements with North and South Dakota for public health purposes. The team also exchanged information and/or tools with Nebraska, Minnesota, and Wisconsin, including discussion of an HIE pilot project with Nebraska in Omaha/Council Bluffs area.

Iowa's implementation project, entitled Continuity of Care Document (CCD): Implications for Private and Secure eHIE, was chosen because of the need in Iowa for greater access to basic patient information, and the opportunity to support future CCD exchange efforts by addressing privacy and security issues up front.

The Privacy and Security Solutions project has also resulted in discussions about governance of e-health activities in the state and the potential creation of a statewide e-health council to oversee activities and funnel resources. State legislators are involved and becoming more educated about health IT, health information exchange, and privacy and security issues.

Interaction with external parties such as RTI, ONC, and other states in the Privacy and Security Solutions project has provided Iowa teams with a much better understanding of national health IT and health information exchange goals and initiatives. The contacts made will continue to benefit the state team's efforts and maintain alignment with national and state directives. The multistate collaboratives and potential health information exchange projects with neighboring states will undoubtedly produce further positive results.

Overall, the groundwork laid during the project will impact future efforts by providing thorough resources and the momentum to carry forward solutions and implementation plans.

#### **4.1.11 Kansas**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In November 2004, Governor Sebelius established the Governor's Commission on Health Care Cost Containment. This commission was charged with recommending solutions to improve patient care through the reduction of duplicative, inefficient administrative processes and developing strategies for efficient and effective uses of health information.

A priority for the commission has been the development of a statewide, shared vision for health IT and health information exchange as the next step in achieving interoperability and the mobilization of information to support patient care across the state. To pursue development of this shared vision, or health information exchange road map, the commission launched the Kansas Health Information Technology State Policy Initiative. Twenty-three Kansas health care industry leaders, including representatives from government, hospitals, physician groups, health plans, employers, academic medical centers, and advocacy groups, were interviewed about the status of health IT and health information exchange in Kansas, health IT's potential to address the state's most pressing health care challenges, and actions necessary to move the state toward broader adoption and use of health IT and health information exchange.

In 2005, the commission retained the services of the eHealth Initiative Foundation to increase awareness of health IT/health information exchange initiatives already under way in Kansas; catalyze and support these efforts; identify health IT/health information exchange adoption strategies (and barriers to those strategies); bring Kansas' experience

into the national policy dialogue; and build a broad Kansas coalition to improve the quality, safety, and efficiency of health care through health IT and health information exchange.

An environmental scan conducted when the Kansas Health Information Technology State Policy Initiative was formed found the following health IT/health information exchange activities in Kansas:

- Central Plains Regional Health Care Foundation's Clinics Patient Index, a shared repository of patient information, linked 6 community clinics in Sedgwick County via a computerized patient enrollment and tracking system through a secure website.
- The Community Health Center (Health Choice) Project, an organization created by community health centers, delegated essential business services that can be more effectively or efficiently operated jointly.
- Jayhawk Point of Care, an integrated solution tied together all of the Pratt Regional Medical Center's key departments in a single database and improved the availability and communication of vital patient information.
- Kansas City Health Exchange's Community Health Record, comprised of approximately 20 of Kansas City's leading employers and health care organizations, developed a business plan for a regional HIE that will govern and manage a Community Health Record for the bistate metro Kansas City area.
- Northwest Kansas Alliance, the largest formal critical access hospital network in the United States, linked members through telemedicine services and expanded them beyond the traditional boundaries of teleradiology.
- Kansas Public Health eXchange (PHIX), a public health initiative in Kansas, created a secure web-based communication system designed for the rapid exchange of public health information between providers.
- KAN-ED, a statewide initiative established by the Kansas state legislature in 2001, provided broadband capabilities to hospitals and other member institutions in the state.
- University of Kansas Medical Center, Center for Telemedicine & Telehealth (KUCTT) pioneered telehealth services to underserved Kansans throughout the state.
- University of Kansas Center for Healthcare Informatics (KU-CHI) was designed to advance the use of health IT by empowering faculty and students with emerging IT toolsets.

Also in 2005, the Kansas Hospital Association hosted several statewide meetings and several subcommittee meetings that led to the establishment of the Electronic Health Record Work Group. This work group coordinated its efforts with the Governor's Health Care Cost Containment Commission and ultimately meshed its goals for health IT and health information exchange with those of the commission. The Kansas Department of Health and Environment (KDHE) was awarded an Information Links grant to work with the Kansas Health Institute, local health departments, KU-CHI, and others to identify best practices in electronically linking public health records with HIEs and legal, administrative, and jurisdictional barriers that present obstacles to the electronic sharing of public health

information. Results of this grant provided guidance to KDHE in creating an electronic linkage between the public health immunization registry in Kansas and the Kansas City Health Information Exchange. Finally, in 2005, the Kansas Foundation for Medical Care surveyed physician offices across Kansas, requesting information about the use of electronic clinical information in their practices.

### *Current Health IT/HIE Landscape*

Kansas made significant progress in the use of health IT and health information exchange with both public and private initiatives under way. The focus of the state's stakeholders is to organize and implement the governance infrastructure required to support, advance, and align the goals of electronic health information exchange projects and initiatives across the state. Recommendations and proposals for such an entity were shared with the governor. Her decision may be rendered by the end of the year. Currently, the governor's HIE Commission—the successor to the Health Care Cost Containment Commission—remains in place.

Several health IT/HIE initiatives have started in Kansas since the Privacy and Security Solutions project proposal was written, including the following:

- Kansas Immunization Registry project (Kansas' custom immunization tracking system)
- KU-Health Informatics Center and CHI's SEEDS project (a collaborative initiative developed to teach nursing and medical school students about health IT and EHRs)
- Community Health Record Pilot in Wichita (to bring Medicaid claims data to the point of care)
- KCCare Link, a shared electronic referral system linking major health care safety net providers to better coordinate and deliver health care to uninsured and underinsured patients

A report by the US Department of Health and Human Services' Office of Inspector General found that Kansas is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Iowa, Louisiana, Mississippi, Vermont, Wisconsin, and Wyoming.)

### *Current Privacy and Security Landscape*

One of Kansas' main activities for the Privacy and Security Solutions project has been developing recommendations for the creation of a coordinating entity in Kansas that would set privacy and security standards not only within Kansas but also between Kansas and

other states. The concept of a coordinating entity in Kansas predates the Privacy and Security Solutions project, originating with a survey performed in 2006 by the Kansas Health Information Technology State Policy Initiative. When the Privacy and Security Solutions project started, its goals aligned perfectly with the intent and direction under way in Kansas at the time, and the work dovetailed with ongoing initiatives as well as planned activities.

In February 2007, due in part to the focus on health IT/health information exchange in Kansas, Governor Sebelius issued an executive order creating the Health Information Exchange Commission (HIEC). When the governor established the HIEC, the initial tasks of the Privacy and Security Solutions project were within 2 months of completion. The HIEC built on the project as well as the governor's statewide HIT/HIE Policy Initiative. The HIEC mandate included a focus on health information security and privacy concerns and a broader focus on promoting widespread adoption of health IT. Several prominent members of the Privacy and Security Solutions project team were appointed by the governor to serve on the Commission. When the Privacy and Security Solutions project was extended in the second half of 2007, the 2 entities continued on complementary and mutually supportive paths.

Using results from the Privacy and Security Solutions assessments and planning tasks, the project team, along with HIEC members, continued work on recommendations for the coordinating entity. In September 2007, by the request of the governor, the HIEC submitted a proposal for the creation of a public/private HIE coordinating entity in Kansas. Members of the Privacy and Security Solutions team reviewed the proposal and largely concurred with its suggestions. This entity, intended to interact with the HIEC and the Kansas Health Policy Authority, would be charged with advancing the use of health IT and ensuring that patients' private health information is protected and secure. Kansas is in the early stages of health IT adoption and health information exchange. By developing a statewide strategic plan for increasing health IT adoption, Kansas intends to mitigate risks of investment while promoting privacy and security best practices.

Continuing work started under the Privacy and Security Solutions contract, the project's LWG produced a catalog of existing statutes and regulations in Kansas that affect health information privacy and security and have implications for the electronic exchange of data. To ensure consistency in data collection processes, a data collection tool was created. The tool was designed to collect laws within the scope of the project, categorize them according to identified topics, and document the general applicability and purpose of the specific law identified.

As preparation for the extension of the Privacy and Security Solutions project (into 2008), collaborative members from the individual state project teams examined terminology and definitions and developed a consistent understanding of the tasks involved in the process of

collecting and assessing statutes involving medical privacy issues. Kansas contributed significantly to this dialogue, having developed and compiled a systematic method for collecting and analyzing the statutes during the project. This process greatly benefited the Kansas efforts as the collaborative discussion considered questions and issues that were then compared with the Kansas assessment tool in the process of evaluating the method, and use of the assessment tool.

The need for consumer education related to privacy and security in health IT and health information exchange was evident to the Kansas team as they worked through the identification of variations in business practices and policies related to the electronic exchange of health information. Consumer education evolved to a major recommendation in the project's solutions and implementation plans and has been identified in the Kansas HIT/HIE Policy Initiative.

Consumers need to have knowledge and information about privacy and security within health information exchange if they are to make informed decisions about their health care. The education, engagement, and trust of consumers are central to the ubiquitous use of health IT as well as a sustainable business model for health information exchange. The Privacy and Security Solutions project provided Kansas a unique opportunity to focus on consumer education in privacy and security. A consumer Education Work Group (EWG) consisting of key stakeholders throughout the state and the bistate Kansas City area has been organized to: (1) analyze market characteristics and select a segment of the market to target in Kansas; (2) develop curriculum content and teaching strategies; and (3) produce instructional materials.

In Kansas, 100 of 105 counties are considered either frontier or rural; therefore, the Privacy and Security Solutions project team decided to focus education efforts on rural customers/consumers. The EWG discussed consumer education and created a content outline initially focusing on specific areas. The EWG also recognized the need to examine existing consumer education materials and adapt those materials to meet the specific needs of the diverse rural populations in the state. To that end, the project team obtained permission from the American Health Information Management Association (AHIMA) to adapt and expand their "train the trainer" campaign for consumer education, "Your Personal Health Information: How to Access, Manage, and Protect it." As part of the education materials, the Privacy and Security Solutions project team is creating a glossary of terms related to privacy and security to assist in educating consumers. By having all trainers use the same definitions for the same terms, Kansas is ensuring that everyone is addressing the subject from the same reference point.

As the EWG was working on this effort, the leaders of the EWG began to work with the project's multistate Consumer Education and Engagement Collaborative to leverage each

state's resources. Several of Kansas' suggestions are being incorporated into the Common Collaborative project and Kansas' individual state portion of the Collaborative.

The Kansas team reported that the most conspicuous outcome of the Privacy and Security Solutions in Kansas has been the engagement of a broad cross-section of stakeholders and policy makers in a discussion of statutory and regulatory reform of privacy and security. This project, as much as any of the state's health IT and health information exchanges, raised the public's awareness of privacy and security within the border context of health information and focused attention on the rights and responsibilities of those who share protected health information. Additionally, many of the staff and leadership of the Kansas project believe that one of the most valuable benefits of the project has been the opportunity to meet with and learn from counterparts in other parts of the country. The Privacy and Security Solutions project enabled Kansas to form multistate collaborations to gain further leverage for their efforts in harmonizing state laws and educating consumers. These collaborations will enable Kansas to develop more effective policy and institutions at the local, regional, and national levels.

#### **4.1.12 Kentucky**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

As a result of collaboration between Governor Fletcher, a bipartisan group of legislators, and the Kentucky Cabinet for Health and Family Services (CHFS), Kentucky passed legislation in 2005 that created a statewide effort to coordinate and promote e-health. This legislation, Senate Bill 2, authorized the creation of 3 entities:

- Kentucky e-Health Network Board, a decision-making body comprising a variety of public and private stakeholders and charged with the development and oversight of Kentucky's e-Health Network
- Kentucky Healthcare Infrastructure Authority, comprising Kentucky's 2 major research universities—the University of Kentucky and the University of Louisville—and charged with performing research and providing expertise in advancing e-health in Kentucky
- Kentucky e-Health Network, a statewide collaborative secure electronic network created to facilitate more accurate, efficient, and confidential sharing of health information

Kentucky's e-health efforts were an outgrowth of many prior technology efforts at the CHFS. These efforts included an integrated public health IT system called the Kentucky Public Health Information Interchange (KPHII). KPHII is the umbrella organization that includes the Kentucky Electronic Public Health Records System and supports multiple public health programs, such as vital statistics, expanded newborn metabolic screening, newborn hearing screening, the statewide immunization registry program, the childhood lead poisoning program, the disease surveillance program, and outbreak management.

Other previous health IT initiatives in the state include Kentucky's new MMIS, a comprehensive and integrated electronic member, provider, and claims management system. Kentucky was also a pioneer in the use of telehealth, creating the Kentucky Telehealth Network, one of the nation's first statewide telehealth initiatives. In addition, to help confront prescription drug abuse in Kentucky, CHFS developed eKASPER, a web-based system for tracking controlled substance prescriptions filled in Kentucky.

Kentucky was participating in a number of grants and contracts related to health IT at the time the Privacy and Security Solutions project proposal was written. Kentucky was a participant in 2 of the 4 pilot projects for the development of an NHIN prototype. The Eastern Kentucky Regional Health Community was included as one of its market sites in the ONC NHIN contract awarded to Accenture. Another ONC NHIN contract was awarded to Northrop Grumman and involved HealthBridge—an electronic collaborative network operating in northern Kentucky and Cincinnati, Ohio.

Kentucky also had a number of smaller e-health projects under way, including the following:

- University of Kentucky—Meeting Information Needs of Referrals Electronically
- Appalachian Regional Healthcare project in Hazard, Kentucky—Connecting Healthcare in Central Appalachia
- Jewish Hospital Healthcare project in Louisville—Emergency Department Information Systems

In January 2006, the Louisville Health Information Exchange (LouHIE) announced the development of an electronic health information system that could provide a unified lifetime health record for all Louisville area residents. LouHIE is a not-for-profit organization governed by a 16-person board of directors representing a cross-section of the greater Louisville community. LouHIE is planning to launch a health record bank that will function like a consumer bank account for health information.

### *Current Health IT/HIE Landscape*

A great deal of health IT/health information exchange activity is occurring in Kentucky that enjoys the strong bipartisan support of the governor and the legislature. In January 2007, Governor Fletcher awarded 5 e-Prescribing Partnerships in Kentucky (ePPIK) grants to assist providers in 14 communities to implement EMRs and use e-prescribing. The e-Prescribing grant program, funded initially by the Foundation for a Healthy Kentucky and the Hal Rogers Grant, promotes the formation of partnerships within a community between physicians' offices, hospitals, pharmacies, and other health care entities to facilitate electronic prescription processing. In September 2007, the governor and CHFS announced a new round of ePPIK grants.

Another collaborative effort is the Kentucky e-Health Summit. The e-Health Summit brought state and community leaders involved in e-health initiatives throughout Kentucky together

to learn more about the efforts of the Kentucky e-Health Network Board and various local health information exchange efforts. The first was held in January 2007, and the next one will be held in December 2007.

Early in 2007, the Cabinet for Health and Family Services (CHFS) and the Kentucky e-Health Network Board also sought passage of HB185, authorizing the creation of a nonprofit corporation attached to the e-Health Board to operate the e-Health Network. In September 2007, Governor Fletcher signed regulations creating the not-for-profit Kentucky e-Health Corporation to advance the state's goal of establishing a statewide electronic health network by 2011. The Kentucky e-Health Corporation will work with the Kentucky e-Health Network Board to develop a statewide network for sharing electronic clinical and administrative information.

The University of Louisville School of Public Health and Information Sciences developed a model curriculum for training privacy and security professionals, specifically in HIPAA and interoperable information exchange. A pilot training session was held November 30, 2007, for 60 CHFS employees from all CHFS business units. A training session was also held at the second annual Kentucky e-Health Summit on December 7, 2007. Both physician and nursing continuing education credits will be available for participation in the Summit training session.

The Appalachian Regional Healthcare initiative is an interstate EHR initiative in Kentucky. Appalachian Regional Healthcare will deploy an EHR system to more than 190 employed and affiliated physicians in rural communities across eastern Kentucky and West Virginia. Another EHR effort took place in Owensboro, Kentucky: in October 2007, physician practices in and around Owensboro linked to a common EHR system that the Owensboro Medical Health System uses for its EHRs.

In addition, the US Department of Health and Human Services awarded Kentucky a \$4.9 million Medicaid Transformation Grant to fund creation of the Kentucky Health Information Partnership (K-HIP) and development of a statewide e-health web portal for exchanging health information. The portal will allow providers to securely access electronic health information, including handling standardized administrative transactions and requests and searching for a summary of a patient's health information. The K-HIP project is a collaborative effort between Medicaid and private payors in the states and is expected to allow access to basic health information, such as a medication list, diagnoses, and lab and diagnostic test history for more than 50% of the residents of the Commonwealth of Kentucky. This project will serve as the foundation for the development of the Kentucky e-Health Network.

### *Current Privacy and Security Landscape*

The Kentucky state team reported several tangible outcomes to the Privacy and Security Solutions project. When the Kentucky e-Health Network Board applied for the project, the board was early in its organizational phase. The project enabled the quick identification of state e-health champions and stimulated an open and continuing dialogue among diverse groups of stakeholders. Interacting with these champions and stakeholder groups has been very useful in moving the board forward and ensuring that Kentucky's e-health efforts are now based on privacy and security best practices. The project also enabled the Kentucky team to interact with their peers in other states, develop a network of contacts, and learn what efforts were occurring in those states.

The Privacy and Security Solutions project has influenced other health IT initiatives in the state. Through its work on this project, the Kentucky team has clearly identified barriers associated with the secure exchange of electronic health information, which can now be used by other groups. Members of LouHIE participated in the state project and, in turn, used some of the findings from the project in their work with LouHIE. Additionally, the University of Kentucky has a network of clinics that have incorporated some of the Privacy and Security Solutions project findings into their work.

The Privacy and Security Solutions project was one of the first projects undertaken by Kentucky's newly established governance body, the Kentucky e-Health Network Board. The project team was charged with informing the board about the effect of privacy and security practices and policies to help establish efficient and effective interoperable health information exchange in Kentucky. Because of the success of this effort, the board formed a permanent privacy and security committee that has been staffed by the Privacy and Security Solutions project steering committee and work group participants.

A central recommendation of the Kentucky Privacy and Security Solutions project team was that user-friendly information on the rules governing electronic disclosure of protected health information, the risks of paper versus electronic medical records, and the positive aspects of electronic health information be developed for the training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators. Additional topics for education include the rules governing health information exchange, the benefits to electronic health information exchange, and their respective rights and obligations regarding enhanced quality of care.

Another result of the project was an in-depth look at privacy and security laws and regulations in Kentucky. The ambiguities between Kentucky and federal law cause extensive confusion and frustration on a daily basis in the health sector. Building on the initial work of the Kentucky team's LWG, a comprehensive HIPAA preemption analysis was developed for use in regulatory amendment activity related to privacy and security issues and for

preparation of future legislation regarding privacy and security of health information. The LWG found that, because definitions related to health information sharing and exchange that presently exist in Kentucky statute are not consistent with the present meaning in paper and electronic environments, analysis was conducted to identify revision definitions related to health information sharing and exchange that presently exist in statute.

After the Kentucky HIPAA preemption analysis and statutory/legislative review process were completed, one important finding was that many impediments that exist to secure sharing of health information by state-regulated facilities could be relieved by amendment of Cabinet's own administrative regulations governing facility licensure. Definitions of a medical record and requirements for storage and retention varied widely and, in many cases, had no applicability to electronic records or transmission of those records. The amendment process is straightforward with legislative and advocacy community oversight. The LWG decided to pursue that course of action in the near term. This direction will gain significant ground for Kentucky and it could be an area of reform that will apply in other states.

The need for facility transfer agreement requirements clarification developed from the original Privacy and Security Solutions work. It was originally believed that there were statutory or regulatory obstacles to transferring medical records with a patient between certain facilities. The legal analysis performed under the original Privacy and Security Solutions grant revealed that belief to be a misinterpretation of the law. The Office of the Inspector General has taken it as an action item to communicate the correct interpretation of applicable law and regulation using a memorandum of understanding authored by the LWG. It was an impediment that turned out to need an educational, not statutory, remedy.

The University of Kentucky's College of Public Health's Department of Health Services Management conducted the analysis of medical recordkeeping requirements in every state health facility licensing regulation to develop the draft regulations, and found great variation in the definition of "medical record," a key concept in defining health information exchange, medical information, and consent. A direct outgrowth of the continuation funding project is the appointment of a workgroup for the development of a single definition of the term "medical record" that can be adapted across facility regulations.

The Kentucky team reported that when the Kentucky e-Health Network Board (KeHN) applied for the Privacy and Security Solutions project, early in its organizational phase, the project allowed quick identification of state e-Health champions. They have found that interacting with various stakeholder groups has been very useful in moving the KeHN board forward and that the project has created an open and continuing dialog with these stakeholders that did not previously exist. The project encouraged Kentucky's team to meet their peers in other states and to learn what other states were doing through regional and national meetings; thus, Kentucky quickly developed a network of contacts.

The project has influenced other health IT initiatives in the state. LouHIE has incorporated some of the findings from the Privacy and Security Solutions project—some members of LouHIE also participated in the project. Additionally, the University of Kentucky has a network of clinics and has incorporated findings of the assessment of variations in business practices into its work.

#### **4.1.13 Louisiana**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In recognition of the importance of advancing health IT to track health outcomes and status more effectively, in 2004 Governor Blanco established the Governor’s Health Care Reform Panel (HCRP) to address Louisiana’s health care issues, including access to health care and improving quality of care. Through the HCRP, the Louisiana Department of Health and Hospitals (DHH) has been able to educate stakeholders such as legislators, health care providers, and interested citizens on the importance of health IT, particularly as it relates to health care quality and monitoring.

When the Privacy and Security Solutions project proposal was written, DHH had made converting to a paperless Medicaid financial eligibility case records system a priority and had made some progress toward this goal. DHH was also preparing to implement a pilot program on electronic prescribing among a group of physicians in training through the use of handheld computers. DHH developed a real-time, personalized decision support tool to prompt Medicaid providers to perform appropriate clinical interventions and preventive care services.

Additionally, Louisiana had been home to a diverse range of partnerships and innovative efforts to employ health IT to improve the health of its population. The following highlights some of the efforts occurring in the state. These projects are based on Louisiana’s efforts with AHRQ’s Transforming Healthcare Quality through Information Technology Grants program:

- The Cardiovascular Care Disparities: Safety-Net HIT strategy focused on cardiovascular disease (CVD) care. Through this initiative, project participants designed a longitudinal CVD information system platform to address disparities in CVD, viewed as a lifelong disease process.
- Distance Management of High-Risk Obstetrical Patients is a project of Woman’s Hospital of Baton Rouge. Woman’s Hospital developed a technology plan to improve access to maternal-fetal medicine services throughout the state and guided the implementation of telemedicine capabilities to provide real-time remote diagnostic ultrasound and consultative services with high-risk pregnancies.
- The HIT Service Integration Planning grant involved safety net providers serving parishes who agree to commit in-kind administrative time and IT staff required to

complete a 1-year planning process, including a detailed assessment of the feasibility of health IT implementation.

- The Louisiana Rural Health Information Technology Partnership focused on health technology in rural areas. The goals of this project were to improve coordination of care, increase quality of care, and provide cost savings to the system.

The occurrence of natural disasters such as Hurricanes Katrina and Rita demonstrated the vulnerability of Louisiana's current system in managing and accessing patient health data and information in a timely and effective manner. The destruction of paper medical records by flood waters and the migration of patients to other states after the hurricanes highlighted the need for complete interoperability. Thousands of individuals were displaced throughout the country, many with health related issues, and had no access to their historical medical records. The paper records were lost in the storm with virtually no hope of recovery. This tragedy could have been largely overcome had health care providers adopted an EHR system with colocated data backup; patients' medical records could have been recovered easily. However, the resistance to EHR adoption because of privacy and security issues (among other issues) means that the state of Louisiana is still living with the reality and vulnerability of a paper-based medical records entity.

#### *Current Health IT/HIE Landscape*

A report by the US Department of Health and Human Services' Office of Inspector General found that Louisiana is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Iowa, Kansas, Mississippi, Vermont, Wisconsin, and Wyoming.)

The rural parish of Pointe Coupee will soon have a more advanced electronic network of medical information than most other areas of the state. Funds awarded by the US Department of Health and Human Services in October 2007 are being used to establish a health IT network in the Pointe Coupee Parish area. The goals of this effort are to improve coordination of care, increase quality of care, and provide cost savings to the system. The \$1.5 million grant will link 11 rural health care providers serving the region. Network members include Pointe Coupee General Hospital, Our Lady of the Lake Regional Medical Center, 4 local rural health clinics managed by Our Lady of the Lake Regional Medical Center in New Roads, Innis Community Health Center, Better Access to Community Health, 2 private practice primary care clinics, and Pointe Coupee Homebound Health and Hospice.

Designated as a health care shortage area for primary, mental health, and dental care, Pointe Coupee Parish has many health challenges. The parish is also considered a medically

underserved area. Although there are 9 private providers locally, 50% of these are near retirement and have greatly reduced their hours of operation. Also, Pointe Coupee General Hospital is the only hospital in the parish and has a total of 25 beds. Establishing an electronic health information network within this system is expected to improve the overall health care system and, more importantly, improve patient care.

Several other Louisiana parishes and communities are working to develop projects or have implemented health IT on a smaller scale. It is hoped that funding opportunities from the federal government will continue to be made available for similar projects in the future.

Louisiana is currently at a crucial moment in its health care redesign after Hurricanes Katrina and Rita. While developing the Privacy and Security Solutions implementation plan, the project management team (PMT) collaborated with stakeholders from the Louisiana Health Information Exchange (LaHIE) and the Louisiana Health Care Quality Forum (LHCQF) Advisory Group, which were both in formative organizational stages.

### *Current Privacy and Security Landscape*

Through the Privacy and Security Solutions project, the Louisiana team found that identification of and alignment with LaHIE and LHCQF would further promote the solutions developed by stakeholders by adding visibility to this process and additional resources. Through the extended implementation plan period, Louisiana's plan was to address privacy and security issues related to governance of health IT/health information exchange implementation and provider/consumer engagements.

Before the Privacy and Security Solutions project, the legal community had only limited participation in privacy and security discussions. Under the Privacy and Security Solutions project, the Louisiana team brought together hundreds of diverse and concerned stakeholders from around the state who were otherwise scattered and isolated. Louisiana has enjoyed high levels of participation from many unpaid volunteers, including attorneys. Louisiana has also been engaged in interstate discussions of privacy and security issues with Florida, Minnesota, Mississippi, and Oklahoma, and formed the Gulf Coast Task Force with Mississippi to address interoperability issues that were brought to the fore by Hurricanes Katrina and Rita.

The Louisiana team suggested the creation of a Louisiana Health IT Resource Center because the adoption of EHRs has substantial clinical and quality advantages compared to traditional paper record-keeping methods. The Privacy and Security Solutions project team in Louisiana pilot tested the process of developing a user-friendly, content-rich, web-based health IT Resource Center and were able to create a successful, functioning web-based center in 6 months.

The Health IT Resource Center is located online at <http://lhcf.org/for-providers/lhit-resource-center>. It contains a speaker database with 4 speakers and information from 3 separate speaking engagements.

Efforts to enroll speakers are ongoing. The website also has 4 white papers and 2 educational brochures. The project has distributed over 2000 of these educational brochures to conference attendees, health care providers, and consumers at various events and conferences held throughout the project period.

In an effort to promote the great strides that have been taken during the past several years by the public sector, private health care facilities, and the vendor community, the Louisiana Privacy and Security Solutions project team cosponsored a conference this fall (initially titled the e-Health Summit Conference) with the local chapter of HIMSS (Health Information Management Systems Society). The purpose of this conference was to promote the advances in privacy and security of health IT and how it relates to the adoption of EHR systems.

The Louisiana Education Awareness Workgroup (EAWG) recruited 3 speakers from different regions of the state to present at the LaHIMSS Conference. Additionally, the EAWG coordinated 1 of the 2 tracks at the LaHIMSS Conference, and 4 of the sessions at the conference were devoted to privacy and security topics. The EAWG also recruited 22 vendors to participate in the conference and provide product and service information to the conference attendees.

In addition to the conference, the Louisiana state project team coordinated several press events to promote the adoption of EHRs and the privacy and security issues related to this effort. Editorials were published in both the *Shreveport Times* and the *New Orleans Times Picayune*. To support these press events and conferences, the Louisiana state project team developed 2 informational brochures that were provided online and in print at these events. These brochures answer many of the frequently asked questions related to privacy and security of EHRs. Two versions were developed, one for consumers and another for providers. Each version was written specifically to the audience in which it was being presented.

#### **4.1.14 Maine**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Maine's initiatives in health IT began in the late 1990s when the Maine Health Information Center led an effort to establish a statewide, coordinated Community Health Information Network (CHIN). Despite great interest and commitment on behalf of providers, the project ultimately stalled as a result of insufficient financial support. However, the CHIN process was not a complete loss. The process entailed the development of technical advisory and confidentiality committees that focused on interoperability and privacy and security protections.

Around the same time, then Governor King established the Year 2000 Blue Ribbon Commission on Health Care, which called attention to increasing health care costs and provided several goals, including the citation of medical records and clinical information as critical objectives to explore in meeting the strategy of “improving the health status of Maine’s citizens.”

In 2003, Governor Baldacci, in a bipartisan partnership with the Maine Legislature, launched the Dirigo Health Reform Initiative. This comprehensive effort was designed to improve access to care and coverage for all Maine citizens, constrain growth in the cost of care, and promote quality of care and patient outcomes. The Dirigo reform effort has established an environment in which local and statewide health IT initiatives can strive to improve the quality of care for Maine’s citizens.

Maine’s statewide clinical information-sharing initiative, the Maine Health Information Network Technology (MHINT), evolved from a 2004 feasibility study funded by a mix of public and private funds. The objective of this study was to assess the readiness of Maine’s health care community in developing a statewide interconnectivity network of selected patient-specific data. Since 2004, MHINT has advanced beyond the project status toward a fully independent, incorporated nonprofit organization. Because an integrated statewide infrastructure for sharing clinical information is so important to the successful reform of Maine’s health care system, the administration has been actively involved in the support of the MHINT initiative.

In addition to the statewide initiatives, many local initiatives have taken place in Maine. Four AHRQ-funded regional initiatives have focused on improving advanced technology systems with the ultimate goal of improving health care quality. The Connecting Maine project, funded by the Robert Wood Johnson Foundation, worked to strengthen the relationship between public health and health care informatics in Maine by extending the strong collaboration between these 2 sectors, joining 2 powerful data integration efforts, and developing a pilot project to link the state and the city of Portland’s public health departments with Maine’s developing health information exchange. The 2 data integration efforts refer to (1) the Integrated Public Health Information System, which implements the PHIN interoperability and data exchange standards and will integrate more than 20 disparate public health data systems under 1 umbrella to collect, analyze, and use population-based data to improve health status; and (2) MHINT, which is well positioned to implement a fully integrated HIE statewide. The Franklin Health Access-RX, funded by the US Department of Health and Human Services’ Healthy Communities Access Project, works to expand access to prescription medications for all residents of greater Franklin County in Western Maine through e-prescription technology. The Franklin Health Access-RX project works closely with all 7 local pharmacies, the Maine CDC, Western Maine Community Action, and other agencies.

### *Current Health IT/HIE Landscape*

Maine continues to develop the health information exchange infrastructure needed in the state, with the state's RHIO, HealthInfoNet, taking the lead. Areas of focus this year have included the development and advancement of a legislative action plan. The primary focus of the plan is to raise awareness of HealthInfoNet among legislators and to obtain funding. Other priorities include clarification of oversight, in response to consumer desire for added penalties for inappropriate disclosures. Possible topics for the 2008 legislative session include clarification of liability and indemnification for HealthInfoNet.

In addition, 2 of the largest health systems have deployed regional picture archiving. The next step in this work is to marry systems together and create a single person identification system. A hospital-based ambulatory record structure has also been developed.

In March 2007, the Maine Medical Center implemented an e-mail security solution to securely share patient records with external specialists, physicians, and medical claims processors. In April 2007, HealthInfoNet selected a partnership to run the complex computer programs underlying the EHR system. Project officials have asked the legislature to pay \$2 million toward the demonstration project, with the remainder expected to come from doctors, hospitals, insurance companies, and other users of the system (Remal, 2007).

In June 2007, the Maine state legislature granted HealthInfoNet \$265,000 to complete a \$1 million grant and bring the total amount raised by HealthInfoNet to \$2.8 million. The money will allow HealthInfoNet to move closer to launching a first-phase implementation of a statewide HIE that will involve participation by the Maine CDC, the 4 largest hospital delivery systems, a rural community hospital, and a major private group practice. The plan is to gather a patient's medical information, which is presently scattered in multiple locations—doctors' and specialists' offices, pharmacies, and emergency rooms—and compile it in a computer database to provide a full picture of a person's medical history using the continuity of care data standard (Huang, 2007).

The presence of HealthInfoNet was a factor in supporting collaboration between competing hospital systems that has now resulted in an executed memorandum of understanding between Maine's 3 largest hospital systems. HealthInfoNet has also taken on some assignments that are significant for the state, such as examining e-prescribing within Medicaid.

HealthInfoNet also serves as a convening body for general health IT and privacy and security issues. The Privacy and Security Solutions project has increased the level of transparency and has allowed consumers to be more empowered. In addition, the project has allowed clinical and technical sides to come together and talk openly.

HealthInfoNet has developed a stakeholder, representative governance structure that incorporates direct involvement by both government and private-sector community

representatives. Although no official legislative mandate identifies HealthInfoNet as the state HIE, HealthInfoNet is included in the state health plan as a critical priority for moving the health delivery infrastructure forward in Maine.

The project has stimulated the creation, advancement, or endorsement of health information exchanges within Maine by presenting the opportunity for building broad stakeholder consensus. More can be done to establish a relationship with all stakeholder groups, and it is an ongoing and active process.

### *Current Privacy and Security Landscape*

The landscape of privacy and security in Maine has changed markedly as a result of this project. The Maine project team brought together individuals from many areas in the state that have a stake in health information exchange and have made great strides working through the complexities that this topic presents.

Building on public/private initiatives begun prior to the project, Maine's project has continued to develop processes of system governance, technical system requirements, consumer engagement while stressing stakeholder involvement and financial support.

The statewide initiative to integrate clinical information (HealthInfoNet) remains the primary goal of health information exchange in Maine. 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. The Privacy and Security Solutions project team supported this effort by identifying several key barriers to the appropriate exchange of health information including:

- a great deal of variability in interpretation and implementation of privacy and security of protected health information by various stakeholders (eg, provider organizations, public agencies, consumers) (identified by the assessment of variation in business practices and policies conducted by the project staff);
- uneven levels of adoption of privacy and security measures, especially in smaller, more rural settings with fewer resources than urban areas;
- lack of knowledge about privacy and security requirements and procedures, particularly among workers one or more steps removed from the collection of protected health information;
- unnecessary withholding of information because of inappropriately stringent interpretation of HIPAA and Maine's privacy laws; although HIPAA was not intended to restrict the release of information, it was sometimes invoked too narrowly and cut off the flow of information when it was actually permitted;
- consistent lack of involvement of consumers; and
- minimal interaction between providers and state public health agencies.

For the 6-month implementation project, the team formulated 2 projects to address several of these issues. In the first, working with New Hampshire, the team identified minimum common data sets to facilitate the exchange of public health and behavioral health data. In the second, the team developed policy to support informed consent for statewide health information exchange and ensure appropriate levels of individual privacy and confidentiality within a sustainable exchange program. Broad stakeholder involvement, a key element of both projects, was a direct consequence of the Privacy and Security Solutions project's approach to the assessment of variations in business practices and policies. The stakeholder groups identified in this assessment have been essential to the success of both projects.

After considerable debate about the work regarding consent, the topic was restated as a question of what constituted informed consent for consumers when addressing the fundamental question of whether to participate in a health information exchange. By concentrating on what it would take to adequately inform a consumer about: (1) the benefits and risks of participation in a health information exchange, (2) the scope of the data to be handled, and (3) who will have access to content under what conditions/context, the team discovered a far more productive framework for considering policy and process options. In fact, by eventually getting to the question of informed consent as the cornerstone of the discussion, the more volatile positions surrounding opt-in versus opt-out were significantly blunted and became more of a question of tactic than a fundamental point of divide. This discovery may aid other states who are working on similar topics.

Privacy and Security Solutions project participants in Maine are using work conducted by other project states nationwide regarding consent forms and policies. Maine is currently making progress toward establishing a consistent patient consent policy and harmonizing consent language to address the opt-in/opt-out issue that exists there. Maine is also in the process of developing a uniform consent form.

Maine continues to work closely with New Hampshire to identify minimum common data sets to facilitate the exchange of public health and behavioral health data. The 2 states have completed their analysis of reportable diseases and initiated discussions with their respective public health departments regarding next steps.

Maine has also been able to engage stakeholders who had previously been left out of privacy and security considerations, such as the Native American nations in Maine, public education, and emergency medical systems. The project has facilitated an increase in the level of interaction with public health and the Veterans Administration. HealthInfoNet, owing at least in part to its involvement in the Privacy and Security Solutions project, is now regarded as the locus of privacy and security expertise in Maine.

In addition to the direct project outcomes, the Privacy and Security Solutions project has allowed clinical and technical representatives to come together and talk openly about privacy and security. This unique environment was created and fostered as part of this

project, and has enabled the team to accelerate progress. The project encouraged Maine to work across states in formulating and implementing privacy and security solutions, particularly in the work with New Hampshire and in quarterly meetings with the other New England States. The team was able to access and use work from other states, which has enabled the team to be more involved and aware of work in other states.

Finally, the Maine project team has seen the project influence other health information technology initiatives in Maine. The Privacy and Security Solutions project has allowed those involved in other initiatives to start thinking statewide rather than just locally. There is also discussion of changing the state's Certificate of Need (CON) law. The proposed changes would have the state include a description of how information system CON applicants will connect to the statewide health information exchange and link to statewide initiatives/plans.

Large health care systems now have a greater understanding of potential issues in their privacy and security procedures and are looking for HealthInfoNet to be a resource. This visibility is now rapidly positioning HealthInfoNet as the de facto source of information for privacy and security issues for health information exchange in Maine.

The team is committed to the overall vision of an integrated statewide clinical information system and will continue to work towards this vision in 2008.

#### **4.1.15 Massachusetts**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

The Massachusetts Health Data Consortium (MHDC), founded in 1978, has provided an infrastructure in Massachusetts for public and private health care organizations to collaborate on health information exchange. MHDC originally created a formal collaboration with the chief executive officers and chief information officers of all health plans, representative large and small hospitals, physicians and other providers, professional societies, and representative nongovernment agencies and departments in the Commonwealth to address health information and data processing issues and efficiencies that would benefit all stakeholders and constituents. MHDC convened early discussions to lay the groundwork for the New England Healthcare EDI [Electronic Data Exchange] Network; created Massachusetts Simplifying Healthcare among Regional Entities (MA-SHARE); has been an early advisor, active participant, and board member of the Massachusetts e-Health Collaborative (MAeHC); and has shared lessons learned with Safe Health.

To respond to HIPAA, MHDC initiated the Privacy and Security Forums in 2000 and a series of HIPAA workshops to provide the opportunity for widespread HIPAA understanding, education, and implementation tools. The forums continue to facilitate new projects to address the requirements, standards, and policies that describe and permit the

interoperability of data exchange. These projects include MedsInfo-ED Pilot, MAeHC's EHR Communities Project, and MA-SHARE's Rx Gateway Project, as well as the Privacy and Security Solutions project.

Massachusetts also had a high level of EHR adoption, at least partly due to the distribution of EHRs by MAeHC in 3 Massachusetts communities. The combination of significant EHR penetration, the relatively advanced stage of exchange, and MHDC's function as a convener organization laid a solid foundation for the Privacy and Security Solutions project.

#### *Current Health IT/HIE Landscape*

Massachusetts continues to have high rates of EHR adoption among providers and functional HIEs. The Privacy and Security Solutions project has created momentum in the health IT/health information exchange environment in the Commonwealth. In addition, the process has shed light on other issues, such as the need for information exchange between primary care providers and mental and behavioral health providers. The information learned as a result of the project has allowed the Commonwealth to take incremental steps forward.

A conference in October addressed the potential integration of physical and behavioral health records. Previously, behavioral health stakeholders were not included in discussions, and the Privacy and Security Solutions project allowed them to be included for the first time. The Massachusetts team believes the conference to be the first of its kind to include both physical health and behavioral health clinicians in discussions about the exchange of health information.

#### *Current Privacy and Security Landscape*

In Massachusetts, the first phase of the Privacy and Security Solutions project identified legal and operational barriers to electronic health information exchange, proposed solutions, and provided a recommended 24-month implementation plan. As a result of the review of barriers, the Massachusetts steering committee concluded that 2 important, yet often understated, challenges to electronic and paper health information exchange exist. First, there is confusion among health care personnel, patients, and consumers about what protected health information and situations require application of federal and/or state privacy laws. The second issue concerns when, how, and where the laws, regulations and entity preferences are applied (particularly those involving sensitive health information). An additional complication is the varying ability of health care provider entities to manage the collection, storage, decision making, and transmission of patient privacy consent information. Accordingly, the steering committee authorized the commencement of the consent management implementation project (CMP). The CMP addresses improvements in electronic clinical data exchange interoperability by identifying the privacy processes, issues, requirements and preferences that drive the decision making to collect, use, and disclose patient information.

The organizing principle underlying the CMP has been that it is difficult to have widespread electronic health information exchange that respects and enforces patients' preferences regarding access to their information without electronic consent management. The CMP was designed to offer greater clarity about the legal requirements for numerous relevant health information exchange scenarios, and to provide, perhaps for the first time, a detailed framework representing the practices, rules and opportunities for standards and harmonization. The framework would then allow protected health information to move between and among providers and appropriate third parties. The project has addressed the identification of consent requirements in a sequenced logical information flow for high-priority treatment scenarios that require protected health information to be transferred across entities, and explored consumer engagement information and education.

The key outcomes of the CMP process include: a use case collection template; use case elements matrix; an online tool for stakeholders to review and comment on use cases; a series of process information flow diagrams that include sensitive health information and public health decision loops; a summary of laws governing sensitive health information in the Commonwealth of Massachusetts; and a working glossary of defined key terms. These tools will be shared broadly across the Massachusetts health care community and can also be used by other states who wish to follow a similar process.

In reviewing the CMP process, the team has reached several important conclusions. First, the information flow diagram allows entities to use their own current practices as starting points. In addition, the model is flexible enough to handle many community standards of rules, rankings and preferences, and supports customization by entities not included in the current project. Thus, the model has the potential to reduce variation by giving new communities the models, templates, and key issues to think about and resolve regarding consent preferences for their entity and their patients. The team also observed that the many differences in laws and regulations do not result in complexities around consent. Rather, they aggregate into a limited number of outcomes and flow switch points. This observation will support stakeholders as they work to operationalize the consent process. Finally, the model was developed to allow for changes and improvements in future technology architecture without major reframing of the model; ie, as technology matures it can be incorporated into the model. Thus, the model will continue to function even as technological advances occur.

With respect to governance and leadership, the Massachusetts Health Data Consortium (MHDC, the state-designated participant in the Privacy and Security Solutions project) has become more visible in the role of convener for privacy and security issues. Of note, MHDC's Security Officers' Forum, established in 2000 to address HIPAA implementation through 2004, will be re-established and re-charged in 2008 to address widespread Massachusetts public and private sector need to collaborate on e-health security exchange issues.

One of the major outcomes of this project has been on stakeholder knowledge and education. The project brought greater clarity about the legal requirements for numerous relevant health information exchange scenarios, and a detailed analysis of current practices and opportunities for standards and/or harmonization in managing patient consent. It also prompted the Massachusetts team to create a consumer and professional educational resource area on a project website to address privacy and security issues around data sharing. The learning that has taken place among stakeholders will support future health information exchange.

The Massachusetts team has identified several key avenues of future work, in addition to participating in the collaborative work groups addressing consent and consumer engagement in 2008. Possibilities for additional work at the state level include:

- Meet with MA-SHARE and technical vendors, including IT resources available from local universities, to take the administrative specifications designed to date and transform them into the functional and technical specifications that could be prototyped and tested.
- Convene the legal subgroup and project team to examine and detail the remaining decision processes for research, public health, and secondary uses of data.
- Determine the best long-term organizational structure to support a commitment to professional and consumer education strategies

These activities will continue to advance secure and private health information exchange within Massachusetts and across states.

#### **4.1.16 Michigan**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Michigan has an unusually diverse population, representing more than 80 nationalities, cultures, and ethnicities, including every socioeconomic group and every major form of health care delivery. Recognizing the importance of extending health IT to all health care settings, Governor Granholm charged the Michigan Department of Community Health (MDCH) and the Michigan Department of Information Technology (MDIT) with finding solutions to barriers that impede adoption of health IT. Subsequently, MDCH and MDIT held stakeholder forums with providers, payers, employers, labor unions, and consumers to hear the perspectives of key stakeholders on the role of state government in health IT policy.

In response to the recommendations of these forums that all stakeholders be involved, the governor, along with the directors of MDCH and MDIT, convened the new Michigan Health Information Network (MHIN) in December 2005. The MHIN brought together more than 300 stakeholders. The group heard from national, regional, and local speakers on the latest developments in health IT and agreed to continue working with the state and other

stakeholders to develop solutions and strategies in developing a statewide health information exchange.

At the beginning of the Privacy and Security Solutions project, 3 RHIOs were based in Michigan. Michigan's Upper Peninsula Health Care Network formed in 1995 and had established a web-based EMR system for 10 rural hospitals, tribal health centers, and mental health agencies to connect them to the area's regional medical center. The Capital Area Health Alliance and its participating partners launched the Lansing area RHIO in November 2005. Southeast Michigan Healthcare Information Exchange had just been started to facilitate access to and retrieval of clinical data to provide safe, timely, efficient, cost-effective, equitable, and patient-centered care.

Several other initiatives also existed in Michigan:

- the Michigan Childhood Immunization Registry (MCIR), an electronic statewide childhood immunization tracking system for children who receive immunizations in Michigan;
- the Michigan Disease Surveillance System (MDSS), designed to facilitate rapid detecting and response to unusual outbreaks of illness that may be the result of bioterrorism, outbreaks of infectious disease, or other public health threats and emergencies;
- the MMIS, an automated management and control system for the Michigan Medical Assistance Program (Medicaid).
- Blue Cross Blue Shield of Michigan's Web-DENIS Provider Portal, a fully functional payer-provider portal;
- Bridges, a multi-agency effort to implement a single, integrated service delivery system for eligibility and benefit determination of Michigan's cash assistance, medical assistance, food assistance, and child care assistance programs; and
- the Michigan Department of Community Health had received one of 2 national awards from the US Department of Health and Human Services' Administration for Children and Families to use data matching of vital records, child support orders, private insurance information available to either parent, and Medicaid eligibility information to ensure that all children involved in court-ordered child support cases that require health care coverage have the best options available.

### *Current Health IT/HIE Landscape*

The Michigan health IT/health information exchange environment is collaborative, innovative, and aggressively moving forward. Michigan received a Medicaid Transformation Grant from the US Department of Health and Human Services to address provider and credentialing issues as they affect health information exchange. The Consortium of Independent Physician Associations (CIPA), a collection of 38 independent physician associations consisting of 4000 physicians in Michigan, will deploy an electronic prescribing technology to 1200 of its members. West Michigan Physicians Network, an organization of 450 physicians representing various medical and surgical specialties and practice sizes,

named a preferred health IT vendor to help it create a communitywide HIE. Blue Cross Blue Shield of Michigan has announced plans to expand its health care electronic data interchange clearinghouse and portal with information on traditional Medicare enrollees.

The Privacy and Security Solutions project encouraged the state team to work across states in formulating and implementing privacy and security solutions. This collaboration has helped make the process far more inclusive. There has been a great deal of sharing of information across states, which has lent much credibility to the Michigan project, in particular with the RHIOs in Michigan. This project has influenced many other health IT initiatives in Michigan. For example, Michigan used scenarios to help broaden the stakeholder population, and these stakeholders have helped shape the governor's blueprint road map to health information exchange, *Conduit to Care: Michigan's e-Health Initiative* (Michigan Health Information Network, 2006).

A fundamental shift in thought processes has taken place in Michigan, including changes in how health IT and health information exchange are viewed. There now exists a much more comprehensive, integrated, valuable, and connected network of individuals and organizations working in this area. Essentially, a whole paradigm shift has occurred.

Prior to the establishment of the Michigan Health IT Commission, people would apply for grants in name of the state without the state's knowledge. Now, all applications must go through the commission, which has provided greater consistency and order in the grants process. The way Michigan now views health IT and health information exchange represents a real shift in the thought process interoperability paradigm. Michigan has now established a process to analyze and propose changes to state laws to support health information exchange (with a focus on privacy and security). The state has also established a formal governance structure for privacy and security. The Michigan Health IT Commission was appointed in August 2006 as an advisory council to the Department of Community Health and the Privacy and Security Solutions project LWG. Their mission is to facilitate and promote the design, implementation, operation, and maintenance of an interoperable health care information infrastructure in Michigan.

### *Current Privacy and Security Landscape*

The barriers to health information exchange identified during the assessment stage by Michigan's LWG included fragmented, conflicting and scattered state privacy and security laws and state laws that are not applicable to health information exchange. The implementation projects that Michigan focused on were the MiHIN Resource Center and the LWG. The MiHIN Resource Center was chosen because the state of Michigan recognized the importance of a centralized body to support and guide the implementation of privacy and security measures in the development of regional health information exchange, a critical component of health care efficiency. The Resource Center supports for Michigan's role as convener and collaborator for health information exchange in Michigan. The state

recognized that a centralized body would have the ability to bring different regional exchange initiatives together by providing parameters, guidelines and support, and bridging gaps between regional efforts in various stages of development.

The LWG's primary goal was to develop a list of priorities, including privacy and security, that the state would address to facilitate health information exchange. In conjunction with providing centralized support to the developing regions, the state also recognized the urgent need for guidance in relation to privacy and security issues surrounding the development of health information exchange. Through the MiHIN Conduit to Care Process, and the first portion of the Privacy and Security Solutions project, Michigan already had a highly effective and cohesive LWG in place. The LWG, made up of attorneys, along with representatives from hospitals, universities, consumer groups, the state and others, was reconvened to continue to build on the work it had already created. The scope of the LWG was limited to: determining the areas of Michigan statutes that needed changes; creating an ordered short list of those priority areas of law based on the need for action; and drafting a position paper detailing those priorities and the reasoning behind them.

The position paper created by the LWG has been completed and was presented to the Michigan's HIT Commission in December 2007. A panel of members from the LWG will discuss the recommendations and answer any questions that the commissioners raise. The commissioners, in turn, will vote on the recommendations and turn over the approved recommendation to the MDCH.

The Michigan Privacy and Security Solutions project has seamlessly incorporated the privacy and security discussion into the health information exchange development process in Michigan. The governance structure originally created for MiHIN is now the coordinating process for all health information exchange-related activities, regardless of the source. Thus, the project has helped created an enduring governance structure and has made privacy and security issues a seamless part of the planning of all health information exchange-related initiatives.

#### **4.1.17 Minnesota**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Minnesota has a long and rich history of health data privacy protections, extending back to 1977. The Minnesota Health Records Act (Minnesota Statutes §§ 144.291–.298) requires patient consent for the disclosure of patient information. Compared to the HIPAA Privacy Rule, and most states, Minnesota law requires written consent even for purposes of treatment, with exceptions existing only for medical emergencies and for disclosures among facilities within an integrated care system. Patient consent generally expires within 1 year.

Through the public-private Minnesota e-Health Initiative, Minnesota is taking a statewide approach to implementing key breakthrough technologies that will empower citizens as health care consumers, inform and connect providers, and protect communities. The initiative is focused on using health IT to produce tangible and specific value to the health consumer that can be realized within a 2- to 6-year period.

A critical component of Minnesota's e-Health Initiative began in 2004 with the formation of a statewide committee to advise the Commissioner of Health on health IT issues and goals. The Minnesota e-Health Advisory Committee has 26 members who represent key sectors, including health care delivery, payers, public health, and consumers. To keep in step with the national progress on health IT adoption, Minnesota e-Health adopted the 4 national strategic goals set by ONC: informing clinical practice, interconnecting clinicians, personalizing care, and improving population/public health.

In addition to the Advisory Committee, Minnesota has created a state-local Minnesota Public Health Information Network (MN-PHIN) steering committee charged with creating the infrastructure and policies that enable timely, accurate, and statewide exchange of public health information. Such a network will enable public health professionals, policy makers, and community partners to respond efficiently and effectively to community health threats, protect the public from serious but preventable diseases or injury, carry out their responsibilities to make Minnesota communities healthier places to live, and enable consumers to access the public health and prevention information they need to make informed health decisions.

Numerous e-Health projects were under way across the state when the Privacy and Security Solutions project proposal was written, including: the Minnesota HIPAA Collaborative (Rx/Medication History Project), the Community-Shared Clinical Abstract to Improve Care, the Winona Health Community Record Data Exchange, the Minnesota InformationLinks, and the Community Health Information Collaborative (CHIC).

### *Current Health IT/HIE Landscape*

Health IT and health information exchange efforts in Minnesota are collaborative, innovative, and strongly supported at the state and local level. In addition to the ongoing initiatives that began before the start of the Privacy and Security Solutions project, recent activities in Minnesota include the following:

- The Minnesota Department of Health's Office of Rural Health and Primary Care announced that it has awarded grants totaling \$3.5 million to help Minnesota providers develop EHR systems. The funding comes from the Interconnected Electronic Health Record Grant Program, a part of the state's e-Health Initiative. The e-Health Initiative is part of a broader set of strategies designed to improve the quality and efficiency of health care.
- The Office of Rural Health and Primary Care is now accepting applications for the Electronic Health Records Revolving Loan Program, which provides 6-year, no-

interest loans up to \$1.5 million on a first-come, first-served basis to help rural and community providers implement EHRs.

- A survey by Stratis Health, Minnesota's Quality Improvement Organization, shows that 63% of primary care clinics have implemented EHRs, a number significantly higher than the national implementation average reported in most national surveys. Adoption in hospitals is nearing 90%, and long-term care facilities are now being surveyed on their adoption of EHRs and related health IT.
- Minnesota's HIE plans to launch early next year an electronic network to enable health care providers and payers to securely exchange clinical information, beginning with patient medication histories, lab orders, and test results and later adding radiology reports, electronic prescriptions and disease surveillance data. When launched, the initiative may be the largest HIE in the country, serving over 3 million people. The HIE is intended to help ensure safer, more effective patient care. Founding partners in the Minnesota Health Information Exchange include Allina Hospitals and Clinics, HealthPartners, Blue Cross Blue Shield of Minnesota, and Medica.

### *Current Privacy and Security Landscape*

The focus of the Minnesota Privacy and Security Solutions project during Phase I was to update the Minnesota Health Records Act to reflect an electronic age. As this law had been amended over time, it became increasingly more difficult to read, had an increasing number of undefined or ambiguous terms, and needed to be updated to reflect needs in an electronic age. For these and other reasons, provider organizations were not always clear on when and how patient consent was to be obtained to disclose health information.

Phase I of the project included these results and recommendations:

- recodified the Minnesota Health Records Act to be more readable;
- provided definitions for new and existing terms such as "health record," "medical emergency," and "record locator service;"
- defined privacy protections and security requirements for a record locator service;
- authorized "representation of consent" so that a provider requesting patient information can attest to the patient's written consent;
- extended liability to a requesting organization that inappropriately request patients' health information (previous liability pertained to the disclosing organization only); and
- required the Commissioner of Health to develop a standardized, universal consent form for a patient to disclose health information, which must be completed by January 1, 2008.

These changes represented the most significant changes to Minnesota's privacy laws in 25 years. The Minnesota Privacy and Security Solutions project team was able to work out over 95% of the privacy issues in the state and incorporate them into the newly recodified and revised Minnesota Health Records Act.

Other legislative outcomes from the 2007 legislative session included a \$14 million appropriation over 2 years to provide grants and no-interest loans to providers seeking to implement interoperable EHRs and related health IT and several key mandates:

- All providers must have interoperable EHRs by 2015.
- The Commissioner of Health must develop health data standards by January 1, 2009, in concert with national efforts.
- The Commissioner must develop a plan to ensure statewide achievement of the 2015 EHR mandate.

As mentioned above, a key priority for the Minnesota project team was developing and implementing a standardized patient consent form for the exchange/disclosure of health information in Minnesota. This form was mandated by the 2007 Minnesota legislature for completion by January 1, 2008. The outcome of the statewide uniform consent project will be a standardized consent form, including both language and format, which can be used universally for obtaining patient consent to disclose/exchange information. Although health care providers are not mandated to use the form, if it is used it must be accepted as legally enforceable by the receiving provider. The Minnesota project team will finish this task by the end of 2007. Minnesota's efforts will be of tremendous benefit to other states considering consent approaches, because they will be able to start from a fully developed model against which to compare each member's own state laws and requirements.

During Phase I of the project, the Minnesota team also developed a framework of 19 health information exchange security principles around 4 interrelated topics that needed to be addressed uniformly to ensure successful electronic exchange. These subsequently became known as the 4 A's: authorization, authentication, access control, and auditing. Work in Minnesota continued on this topic throughout the project and will continue in 2008. The desired outcome for the security principles project is to implement, document, and refine 4–5 of the most important of the 19 security principles in active regional health information exchanges, and to develop various tools (models, checklists, guidance documents) that can support others (in and outside of Minnesota) to implement changes based on the principles. This case study approach is necessary because the 19 principles are currently at a fairly high level and not prescriptive in approach or best practices. The case studies will enable existing HIEs to develop mechanisms for incorporating the most critical security principles into their health information exchange development activities.

Work on the Privacy and Security Solutions project led to additional outcomes in Minnesota. Changes to the privacy laws, discussed above, have encouraged both statewide and regional exchange projects by addressing their uncertainty over consent requirements and the legality and liability of the record locator service. The Privacy and Security Solutions project encouraged the Minnesota Department of Health to work across state lines in formulating and implementing privacy and security solutions through the collaboratives,

such as the standardized consent form. The project led staff to engage stakeholders, including privacy advocates, at a more in-depth and concrete level, which led to more actionable results. A formal governance structure for privacy and security was established within the state. The Minnesota state project team worked out more than 95% of the privacy issues in the state and incorporated them into the newly recodified and revised Minnesota Health Records Act. Security issues are handled less formally with the e-Health Advisory Committee and a Minnesota HIMSS group of chief information officers that meets monthly to talk about security issues. Such forums address complex issues such as breach notification. The Minnesota state project team continues to address both state and national security and privacy issues under the aegis of the statutorily established Minnesota e-Health Initiative and its 26-member advisory committee. Involvement as a Privacy and Security Solutions–funded project enabled Minnesota not only to update its privacy laws but also to respond more readily to new legislative mandates, such as the standardized consent form and instructions. Collecting sample forms and recruiting attorneys and others to serve on a working committee has been much easier owing to Minnesota’s successful history and experience with the Privacy and Security Solutions project.

Participating in the Privacy and Security Solutions project has led the Minnesota team members to work with stakeholders at a detailed, in-depth level that had not been possible previously. In particular, the project has resulted in an increased interaction with privacy advocates. Not only has Minnesota been able to update its privacy laws, but the state has also responded more readily to new legislative mandates, such as the standardized consent form and instructions. Collecting sample forms and recruiting attorneys and others to serve on a working committee has been much easier because of Minnesota’s successful history and experience with Privacy and Security Solutions project.

#### **4.1.18 Mississippi**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

The aftermath of Hurricanes Katrina and Rita in 2005 highlighted the vulnerability of the current paper-based medical record systems. Medical records for a large number of Mississippi’s evacuees were destroyed or misplaced, resulting in disruption of both routine and emergency medical treatment—an outcome that led to calls from many sectors for an integrated health information network that offered availability while maintaining privacy and security. As the recovery process began, Governor Barbour established a commission for “Recovery and Rebuilding—Building Back Better Than Ever,” to make recommendations for recovery efforts in the coastal area. Among other things, the commission recommended extending health IT, such as EHRs, to all providers.

Under the program for the *Digital Health Recovery for the Gulf Coast*, ONC developed contracts with the Southern Governor’s Association and the State of Louisiana Department

of Health and Hospitals to promote the widespread use of EHRs in the Gulf Coast regions affected by Katrina and other recent hurricanes. The association hosted a Gulf Coast Health Information Task Force, which brought together local and national resources to coordinate planning to help physicians, hospitals, and other health care providers to rebuild an electronic medical information structure.

Information & Quality Healthcare (IQH), the Medicare Quality Improvement Organization for Mississippi and the governor's designee for the Privacy and Security Solutions project, performed an environmental scan as part of the DOQ-IT project in November 2005 to assess the extent of penetration of information technology and EHRs throughout Mississippi. IQH estimated that 10% of rural hospitals have some form of electronic information systems. However, they reported that all urban hospitals are using electronic information systems for various functions and that the larger hospitals have some form of shared clinical information systems.

In separate studies, IQH and several partners conducted a survey of physicians to assess the degree of use of health IT in the state. In the survey of physician offices, the findings reinforced that Mississippi is dominated by small practices. Information gathered by IQH staff revealed that, given this predominance of small practices, vendors are likely to be slow to penetrate the market with the high acquisition costs relative to the profit and market size. IQH staff also observed a lack of technical staff at the practices to assist with EHR selection and servicing after implementation.

The University of Mississippi Medical Center (UMMC) in Jackson is the health sciences campus of the University of Mississippi. The Patient Safety and Surveillance Center was established by UMMC to improve patient access, safety, and care among Mississippi's rural and underserved populations. The center has received funds to help develop web-based event and medication error reporting systems. As part of this initiative, the center created a RHIO, with 8 rural hospitals participating.

The North Mississippi Health Services (NMHS) is a diversified regional health care organization that serves 22 counties in north Mississippi and northwest Alabama from headquarters in Tupelo, Mississippi. The NMHS organization covers a broad range of acute diagnostic and therapeutic services through its participating members. The North Mississippi Medical Center in Tupelo began laying the framework for its EHR in the early 1980s. Starting in 1999, NMHS transformed paper records to EHR in its clinics. Since then, its information system has evolved into a single all-inclusive interoperable EHR that serves all of its hospitals, clinics, home health agencies, and nursing homes. This transformation has grown to include clinics not owned by NMHS, which has essentially allowed the creation of an electronic community health record.

### *Current Health IT/HIE Landscape*

IQH, the governor's designee for the Privacy and Security Solutions project, has a 35-year history as the Medicare Quality Improvement Organization for Mississippi. By serving as a resource to the state's health care providers and to Medicare beneficiaries, IQH and the State of Mississippi seek to fulfill the vision of being a leader in promoting a quality and cost-effective health care system. IQH joined the Foundation for eHealth Initiative and the HIMSS effort, recognizing the opportunity to be a part of a wide range of disciplines that are working toward improving health care through information exchange and technology.

The Foundation for eHealth Initiative conducted a preliminary assessment in 2006 of health information exchange in Mississippi. This preliminary assessment found that 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 personal health information is limited by the lack of connectivity, health IT integration, trained IT personnel, and funding. For more information about the status of statewide HIE in Mississippi, see the website (eHealth Initiative, 2007).

The widespread adoption of health IT and health information exchange among Mississippi's health care providers continues to progress. Health IT is being used primarily in urban settings throughout the state, typically centered on medical facilities. Several of the larger medical institutions have implemented EHR systems that could serve as the foundation for the development of a RHIO.

A number of initiatives in the public and private sectors also highlight efforts to facilitate the widespread use of health IT to improve the safety and quality of health care. Examples include the Medicaid Pharmacy Point of Sale system, the Department of Health's immunization registry and infectious disease surveillance systems, the University of Mississippi Medical Center's efforts to assist the rural and underserved regions of Mississippi through its telemedicine and health information exchange programs, and the initiatives of IQH, such as its DOQ-IT program and the Katrina Phoenix project, both of which are helping to promote the use of health IT by health care providers.

Following are some examples of recent state activity:

- Governor Haley Barbour issued Executive Order 979 in March 2007 creating the Mississippi Health Information Infrastructure Task Force. The executive order specifically directs the task force to review issues about the creation of a statewide and interstate health IT infrastructure to improve the quality and safety of health care delivery in Mississippi. The mission of the task force is to develop and advise the governor of an overall strategy for the adoption and use of health IT and health information exchange to improve health care in Mississippi. It is the vision of the task force that all providers adopt EHRs and other useful information technologies and that there be a reliable, trusted, secure system to facilitate the exchange of health information in Mississippi.

- The governor's office secured a grant to establish a community health data exchange involving the 6 coastal counties along the Gulf Coast to restore the health information system that was damaged by Hurricane Katrina. The grant will create a network for sharing electronic health information and assist with technology adoption by providers.
- In January 2007, the Mississippi Division of Medicaid received funding from the CMS Medicaid Transformation Grant program that will be used to help establish a statewide patient-focused electronic health information system for sharing health data with Medicaid, other state agencies, and providers.
- Natchez Regional Medical Center, a 179-bed hospital, will implement a subscription-based EHR and forms automation system.
- South Mississippi Urgent Care (SMUC) is working with Austin, Texas-based vendor PracticeIT, which specializes in EMRs and handheld diagnostic devices, to complete its move to electronic records. SMUC has 2 locations and plans on opening 2 more this year. The next clinic was scheduled to open in Biloxi in October 2007.

A report by the US Department of Health and Human Services' Office of Inspector General found that Mississippi is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Iowa, Kansas, Louisiana, Vermont, Wisconsin, and Wyoming.)

### *Current Privacy and Security Landscape*

The biggest impact of the Privacy and Security Solutions project in Mississippi has been the formation of a statewide network comprised of more than 150 stakeholders focused on the secure and private transfer of health information and committed to resolving attendant issues that promote electronic health information exchange while protecting patient information. The Privacy and Security Solutions project helped raise awareness of privacy and security issues in Mississippi and identified a large community of stakeholders. It created opportunities for participation among stakeholder groups that previously had little or no participation in projects of this size and scale, and the project increased information sharing among consumers and consumer advocacy groups.

The Mississippi team's Final Assessment of Variations and Analysis of Solutions Report concluded that business practices of various stakeholders resulted from misinterpretation and confusion in the application of HIPAA regulations. The report also concluded that health care consumers do not understand privacy issues. Both of these conclusions point to the need for education about health information technology in the state. Solution #5 of the team's Final Implementation Plan Report provides a road map for the development and implementation of professional and consumer educational materials. Educational topics

include the secure exchange of health information, ethics in health care, and health care identity theft. The implementation plan strives to create avenues of communication and provides much-needed educational opportunities for all areas of the state.

The Privacy and Security Solutions project raised awareness of privacy and security issues in Mississippi and identified a large community of stakeholders. The project brought together over 150 stakeholders interested in the secure and private transfer of health information, and created networking opportunities for stakeholders who previously had little or no involvement in projects of this size and scale. The project also increased information sharing among consumers and consumer advocacy groups.

The project convened stakeholders in all areas of practice to work together on the assessment of variations, analysis of solutions, and implementation strategies identified during the first phase of work. These work groups have continued to work together and are essential in sustaining health information technology initiatives in the state.

The Privacy and Security Solutions project provided additional impetus for the formation of the Governor's Task Force, which included a specific charge to ensure health information privacy and security in electronic health information exchange. Lack of a centralized authority to oversee the implementation of secure, integrated interoperable health information net and infrastructure was one of the barriers the project identified in the Assessment of Variations and Analysis of Solutions Report. The Governor's Task Force will produce a road map that may lead to a centralized entity for the governance of privacy and security issues in Mississippi.

Interest generated by project's activities and reports on the level of health IT and health information exchange in Mississippi and collaboration with the Governor's Task Force have formalized into a cohesive working partnership. One of the project team members now

serves as the chairman of the Education/Communication Work Group; the project director and the project coordinator serve on the Governor's Task Force Privacy; and Security Work Group, and the co-chair of the Governor's Task Force is the president of IQH.

The Privacy and Security Solutions project encouraged collaboration across state lines in formulating and implementing privacy and security solutions. The Mississippi project team is a member of the multistate collaborative that includes Michigan, Kentucky, Florida, Wyoming, Tennessee, and Louisiana. Mississippi has begun to undertake cross-state initiatives, continuing to work closely with Wyoming on provider education issues, and has learned from states with more health IT adoption and active exchange in advance of expanding these efforts in Mississippi.

#### **4.1.19 New Hampshire**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In 2001, the Dartmouth-Hitchcock Medical Clinics began deploying Patient Online (POL) at its Manchester and Nashua divisions. POL enabled patients to request appointments and prescription refills, send messages to providers, update demographics and insurance information, and download medical forms via a secure website.

Several events occurred in 2005, just prior to the start of the Privacy and Security Solutions project. Governor Lynch convened the Citizen's Health Initiative to create a system of care featuring health promotion and disease prevention activities, improved quality of health care; and transparency of information. To reach these goals, the governor identified and convened a comprehensive stakeholder community of more than 150 people from a broad range of health care, business, government, and consumer groups.

In November 2005, the University of New Hampshire convened the first statewide summit to explore the creation of a statewide, interconnected health information system. The summit, sponsored by the Citizen's Health Initiative and funded by local payers, was attended by providers, payers, government, citizen groups, legislators, quality organizations, academics, business leaders, and technology providers. The summit led to the creation of the New Hampshire Health Care Interconnectivity Project in January 2006 to supplement the health data collection and analysis effort under way by the initiative and to provide a comprehensive picture of the health of New Hampshire citizens and the care they receive.

The Capital Region Healthcare Corporation entities completed a planning project for the "Electronic Communication Across Provider Setting (ECAPS)" project, awarded under AHRQ's Transforming Healthcare Quality through Information Technology Grants program. The project resulted in an implementation plan for exchanging office-based patient record data and site preparation for software enhancement in 2 rural settings.

In 2005, practices in New Hampshire and Vermont received funding from AHRQ for a project called “Constructing Rural Health Information Systems: Imposing Interoperability on Disparate Legacy Information Systems, Developing Electronic Health Records, and Connecting Rural Healthcare Providers.” The consortium identified an EHR system that has been shown to succeed in this task.

The New London Hospital received an award in 2005 from the loan/grant program of the US Department of Agriculture Rural Development Office for to implement a telemedicine system, designed to advance patient service, quality, and safety. The system will provide access to patient information to all clinical staff and health care providers in the hospital and in physician practices, school-based health clinics, outpatient services, and nursing homes.

The New Hampshire Department of Health and Human Services (DHHS) sponsored 2 projects—the Community Health Profiles and the New Hampshire Comprehensive Health Information System—to provide health information from claims paid on all New Hampshire residents covered either by a private insurance carrier or by Medicaid. The New Hampshire Information Center at the University of New Hampshire provided project support to DHHS in the development of a web-based reporting and query system that provided information on the health of New Hampshire’s communities for use in program development, community planning, and research. DHHS supported the Syndrome Tracking Encounter Management System and the Communicable Disease Surveillance System to support enhanced early-detection capacity for outbreaks and conditions of public health importance. Finally, the state developed the Automated Hospital Emergency Department Data (AHEDD) system, a mechanism that automated daily data collection from all New Hampshire hospital emergency departments to support state public health program surveillance to provide DHSS with real-time emergency department utilization data. By early 2006, nearly half of New Hampshire’s hospitals were using the AHEDD project.

New Hampshire began the Privacy and Security Solutions project with significant technological infrastructure: more than half of all New Hampshire providers have electronic health records (compared with about 25% nationwide), and all of New Hampshire’s federally qualified health centers have electronic health records. This infrastructure, combined with New Hampshire’s libertarian leanings and lean tax structure, represents a unique environment.

### *Current Health IT/HIE Landscape*

New Hampshire continues to develop its health IT/health information exchange environment and to build stakeholder support. Recent activity includes the governor’s ePrescribing project, which is being managed by the Citizen’s Health Initiative. New Hampshire’s ePrescribing project has the goal of providing ePrescribing technology for all prescribers by October 2008. The initiative led a statewide work group in the summer of 2007 that developed a vision and principles document meant to drive health IT/health information

exchange purchasing decisions between now and 2014. The document was ratified in September 2007 and will lead to the development of a statewide strategic plan in 2008.

### *Current Privacy and Security Landscape*

In the initial phase of the Privacy and Security Solutions project, the New Hampshire project team identified 3 major areas for action. First, in its legal review, the state found that the law governing the privacy of medical records had several key gaps, and was insufficient to support electronic health information exchange. To support the creation of new legislation, the team drafted a statement of vision and principles to guide amendments to the law. Second, given the extensive existing infrastructure, the state decided to review third party consent and security policies. Finally, the New Hampshire team examined the feasibility of exchange of public health data with Maine, as a natural disaster could easily require such an exchange.

The project team found that state law, specifically N.H. Rev. Stat. Ann § 332-I, broadly states that the information contained within an individual's health record is the personal property of the individual. New Hampshire is in a minority of states in this regard. The law does not define health information, what it can be used for, and by whom, and does not address these issues relative to the disclosure and exchange of personal health information. To address these shortcomings, the team decided to develop revised legislation relative to medical records privacy and security. The revisions stem from the assessment of variation in business practices and policies related to privacy and security. The team also developed a vision and principles statement that recognized that security and privacy are paramount to all health information exchange activities.

In New Hampshire, legislation is typically drafted by legislators and submitted to the General Court, with the details hammered out in committee, with lobbyists, and on the floor. The Privacy and Security Solutions team took a different approach with their proposed revisions, due primarily to the complexity and multiple nuances of the issues. The team convened a multistakeholder privacy and security work group facilitated by staff from the New Hampshire Citizens Health Initiative and the Privacy and Security Solutions project. This work group comprised legislators and special interest groups who would be responsible for implementation of the legislation—primarily health care providers. The team identified philosophical differences of opinion on the issue of sharing of medical information between clinicians and privacy advocates. The clinicians voiced the need to have access to a patient's entire medical record to enable the level of quality related to clinical decision making while privacy advocates sought limits to the amount of information shared in some cases, and viewed their right to privacy to trump the clinical need for information. The draft legislation proposes to resolve this issue through provider indemnification as well as the future ability to segment portions of the medical record more effectively.

The draft legislation to revise N.H. Rev. Stat. Ann § 332-I was submitted for the 2008 legislative session on November 2, 2007. The legislative session begins in January 2008 and runs through June 2008. The privacy and security work group continues to convene stakeholders to discuss the legislation as presented and develop legislative strategy and input. The bill currently has bipartisan sponsors from the House and Senate.

Key provisions of the proposed legislation include:

- reaffirmation of patient's ownership of medical record content;
- patient's right to copy of record;
- patient's right to request amendment of medical record;
- patient's right to accounting of all disclosures of protected health information;
- patient's right to audit trail of access to HER;
- universal disclosure form is in effect until revoked orally or in writing by the patient;
- opt-out for clinical information disclosure;
- opt-in for research use
- opt-in for commercial use;
- establishment of legal structure for a future HIE entity;
- providers required to treat patient even if patient refuses to allow disclosure;
- break the glass at provider's clinical discretion;
- provider indemnification if patient withholds information and adverse event occurs;  
and
- commission created to develop the universal disclosure form and education/outreach strategy.

The draft legislation requires the creation of a universal disclosure form that patients would sign in their provider office to state their preferences. This form has also been drafted. Overall, these revisions represent a substantial change to New Hampshire's existing laws. However, the articulated vision and principles will assist in determining how the law should be implemented.

Another key component of New Hampshire's implementation plan has been a review of third-party consent and privacy policies. In the first phase of the Privacy and Security Solutions project, the team noted that many health information exchange activities occur through third-party vendors and facilitators for such data as electronic medical records, e-prescribing, disease management, and other clinical systems. Given the widespread use of such vendors, and the possibility of future requests for proposals related to health information exchange, New Hampshire reviewed the security and privacy policies of potential third-party health information exchange providers and payers. The review has led

to a broader understanding of current privacy policies within the state, and a template should subsequent review be necessary. The review will also be used to inform future requests for proposals related to health information exchange.

The New Hampshire project team also examined the development of a minimum data set for the communication of public health events and associated issues of privacy, security, and legality. Privacy and Security Solutions project teams in New Hampshire and Maine worked collaboratively to assess reportable public health events in each state and their thresholds for reporting. These matrices were then compared and synthesized and a legal review conducted (currently ongoing). This work will result in a template for making cross-border assessments.

New Hampshire Connects for Health, the statewide health information exchange planning project, has begun moving into its second phase of foundational planning. The Privacy and Security Solutions project laid the groundwork by developing privacy and security criteria and principals, draft legislation related to the privacy of personal health information, and a draft universal consent form. These, in turn, are helping to form the basis for New Hampshire's strategic plan for health information exchange and shared health information exchange vision and principals as well as the state's first health information exchange pilot project in the North Country.

The project also facilitated future development of health information exchange. An analysis of the need for health information exchange is underway in the North Country, the rural northern part of New Hampshire, and to determine the financial viability of a North Country regional health exchange effort.

A group was convened in May 2007 to draft the vision statement and principles (see following paragraphs), which were then ratified by the New Hampshire Citizens Health Initiative in September 2007. The New Hampshire Citizens Health Initiative is a public-private partnership that works to promote safe, quality, and effective health care for all New Hampshire citizens. These principles formed the foundation for the legislation drafted by the project team and will continue to inform work at the state level. These principles will also offer a point of reference and perspective should the proposed legislation eventually be litigated.

- *Vision Statement for New Hampshire Health Care Information Technology and Exchange in 2014:* For health IT and health information exchange to be successful in New Hampshire, there is a need to recognize the interrelationships and importance of patient privacy, patient safety, and public health. The New Hampshire Citizens Health Initiative holds the following vision for health care information technology and exchange for 2014:
- **Private and Secure.** A patient's personal health information will be secure, private, and accessed only with patient consent or as otherwise authorized or required by law.

- **Promotes Quality, Safety, and Efficiency.** Health IT and health information exchange will serve as vehicles to promote quality and patient safety, increase efficiencies in health care delivery, and improve public health;
- **Electronic.** All health care providers will use a secure, electronic record for their patients' personal health information;
- **Accessible.** All patients will have access to a secure, electronic, and portable health record;
- **Equitable.** Health information exchange will be a vehicle to support equitable access to health care services.

The Privacy and Security Solutions project resulted in the coalescence of a core team of experts that will continue to address the state's issues of privacy and security in a variety of settings over the next few years. Commitment from the New Hampshire Citizens Health Initiative and the governor's office has been secured to continue to work towards a statewide plan for health IT and health information exchange. Future opportunities include plans to develop a statewide, long term strategic plan for continuing investment in health information technology and health information exchange, which will be completed in 2008. The project team is also assessing the feasibility of developing a revolving loan mechanism to assist independent physician practices in affording electronic health record systems. The team also plans to develop a consumer engagement and education strategy regarding privacy and security of medical information, should the legislation pass in 2008. Finally, New Hampshire continues to develop partnerships with Maine, Vermont, and Massachusetts given that New Hampshire is geographically bordered by these 3 states and they currently have active health information exchange initiatives in various stages of development.

Overall the New Hampshire team has identified 4 key outcomes that would not have been possible without the Privacy and Security Solutions project. The resources brought to bear by the federal government have allowed New Hampshire to:

- accelerate legislative progress,
- document the current challenges,
- interact with other state counterparts, and
- begin to develop a road map for statewide health information exchange efforts.

New Hampshire will continue its work with the consent collaborative in 2008, and work to further define the ways that New England states can work together on the issues of privacy and security.

#### **4.1.20 New Jersey**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

New Jersey's active interest in electronic systems as a means of increasing health care quality and reducing costs began in 1993 when the New Jersey State Legislature, with the concurrence of the governor, asked Thomas Edison State College and the New Jersey Institute of Technology to conduct an 18-month study analyzing current methods, barriers, and recommendations for achieving savings and administrative simplification in the New Jersey health care system. This project became known as the Healthcare Information Networks and Technology (HINT) study and included a statewide survey on administrative costs, barriers, and privacy issues; the creation of a HINT Advisory Council, which was a public-private collaboration representing a cross-section of health care entities; and focus groups. The HINT study contained many of the same recommendations that ultimately were included in the administrative simplification section of the federal HIPAA law of 1996.

By 1999, New Jersey had adopted the HINT law, which required the New Jersey Department of Banking and Insurance (DOBI) to adopt rules for the deployment of the HIPAA electronic transaction and code set (TCS). DOBI realized that the HINT Advisory Council working model created in 1993 would serve as a useful platform for a successful implementation of HIPAA's TCS and that a voluntary association of public and private parties would serve as an invaluable resource from which DOBI could gather technical information and develop implementation plans. Consequently, the New Jersey DOBI HIPAA/HINT Task Force was formed to undertake the primary role of identifying, contacting, convening, and organizing the interested and necessary parties into useful work groups. The work of the task force, and DOBI's role, has been to bring the participants together in a cooperative working environment so they can take the necessary steps to make these complex electronic systems work more effectively. On January 12, 2006, the HINT Law was amended and directs DOBI, in consultation with the New Jersey Department of Health and Senior Services and Thomas Edison State College, to adopt rules and regulations for the development and deployment of EHRs in New Jersey.

The DOBI Task Force formed an EHR work group to develop demonstration programs by which stakeholders will access a common electronic platform with appropriate privacy and security measures for the exchange of information found in the health records maintained by providers and payers in a region. The task force held general conferences in May and November 2005 and formed a cooperative relationship with many stakeholders in the state. DOBI used the task force as the nucleus for identifying the necessary stakeholders to work on the Privacy and Security Solutions project.

### *Current Health IT/HIE Landscape*

New Jersey has been developing its health IT/health information exchange capabilities since the mid-1990s, along with the academic community. The environment is inclusive, receptive, and collaborative.

Recently, the New Jersey Assembly passed legislation to enhance the quality of health care delivered to New Jersey residents through a health IT system. The New Jersey Health Information Technology Promotion Act (A-4044) would establish the state's first EMR infrastructure and create a Health Information Technology Commission to oversee the development, implementation, and oversight of the program. The bill has passed the Assembly, and the Senate plans to hold subsequent hearings to discuss amendments to the bill. The Senate bill is forecast to include amendments that will add implementation steps to the Assembly version, which only called for additional study of health IT issues.

The legislation references the Privacy and Security Solutions project work as a foundation for the proposed state law. The proposed legislation also calls for a public-private partnership to develop e-health and health IT in New Jersey and will create a self-sustaining structure. Separately, the hospital association and Blue Cross Blue Shield of New Jersey have assembled a task force to develop an implementation plan and requirements for a RHIO. The report and feasibility study will likely be part of the proposed legislation. One full-time employee now works exclusively on coordination of EHR development. Proposed legislation will also create a state Office for Electronic Health Information Technology, with necessary supporting staff.

Recently, the commissioners of banking and insurance, health and senior services, child and family services, and human services met with the state IT director and chief information officer for Medicaid to form the governor's Health Information Technology work group. This group is charged with the responsibility to harmonize the efforts of all state agencies to advance health IT in New Jersey. In addition, a policy decision has been made to proceed with EHR development.

The executive branch is also involved in health IT and health information exchange initiatives. Governor Corzine has established the Commission on Rationalizing Health Care Costs. The commission includes an IT infrastructure committee that is studying issues related to EHRs and will make recommendations to the governor by the end of 2007. The commission plans to publish a report in 2007 that will include a chapter on EHRs and EHR systems.

An office for the development of EHRs/health IT has been established within the New Jersey Department of Banking and Insurance to provide leadership at the state level. The state's first RHIO was created in Cape May and Atlantic Counties. A feasibility/business plan for a

state hospital records RHIO, supported by the NJ Hospital Association and Blue Cross Blue Shield of New Jersey, has been developed.

In addition, New Jersey Medicaid applied for and received a Medicaid Transformation Grant to start developing EHRs for Medicaid children. New Jersey has also submitted a proposal to CDC to conduct a demonstration project on sharing information with a patient, the patient's parents, and the clinician.

New Jersey met with New York City and New York State to create electronic, Internet-based, open source immunization registries. Immunization registries have national standards in place. Bulk transfers of immunization data have occurred between New York City and New Jersey, and data-sharing agreements are being drafted. New Jersey and New York City have successfully demonstrated batch exchange, and memoranda of understanding to support interstate harmonization of immunization registries have been drafted.

Other developments will also impact health IT/health information exchange in New Jersey. The state has recently adopted rules that require health care payers to use health care clearinghouses only to handle electronic HIPAA transaction and code sets that are accredited as to privacy and security (N.J.A.C. 11:22-3.8). In addition, a new RHIO has been formed in South Jersey, in Atlantic and Cape May counties. SJMRX, the South Jersey Medical Record Exchange, may be the site of beta testing for a statewide RHIO.

A formal governance system is still evolving. It may become more formal when state legislation is enacted, and all stakeholders are working toward consensus. The Privacy and Security Solutions project has been the initiating event for this activity. Finally, the project has served to stimulate the creation of HIEs, such as the South Jersey RHIO. The state team also expects more development in the near future as health IT becomes a greater priority at the state level.

#### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project has generated substantial interest and desire in all facets of the health care industry to take the next necessary steps in the transition from paper-based record systems to widespread use of EHRs. The Privacy and Security Solutions project linked otherwise divergent interests to the significance of privacy and security and triggered an immediate commitment to move forward with health information exchange in New Jersey. The assessment of variation in business practices and policies in health information exchange highlighted the confusion and different interpretations of HIPAA and other requirements that currently exist in New Jersey. Each department in state government enforced its own laws and regulations without any thought of harmonization or consistency of application. Health care providers and others handling health information

consequently developed different and sometime conflicting practices. This variability was identified as a barrier to interoperability.

The state's Final Implementation Report reached similar conclusions: that there was considerable misapplication of the HIPAA privacy and security regulations. The project team proposed, among other measures, a New Jersey-based education program directed toward providers and consumers to ameliorate the confusion about privacy and security laws and regulations.

The project team also learned that protected health information found in public health registries was not being shared across state lines because of unresolved issues of privacy and security. The team has proposed meetings with public health agencies in adjacent states to develop linkages among public health registries.

To address misconceptions of state and federal law, the project team in New Jersey developed 2 different versions of materials for providers and consumers. The team began making presentations to groups of providers and consumers in December 2007, and will continue to do so through the Department of Banking and Insurance's Speakers Bureau.

New Jersey is currently engaged in creating interoperable interstate immunization registries with New York State and New York City. Technology has not been a significant barrier to implementing this interstate exchange. Rather, the privacy and security barriers that are erected around state territorial boundaries have been issues in developing multistate immunization registries. The team's current work in the implementation phase has demonstrated that the states can create and execute mutually agreeable memoranda of understanding and data sharing agreements to address and resolve these impediments.

In addition to the project work, New Jersey has also received a Medicaid Transformation Grant to create a single electronic health record for Medicaid-covered children that will be interoperable over state lines. This grant has been awarded to the New Jersey Department of Health and Senior Services (NJDOHS); NJDOHS has asked the Privacy and Security Solutions project team to assist with privacy, security, and composition of the records.

The team continues to interact with New York State Department of Health to harmonize the public health electronic reporting registries that currently exist separately in New York and New Jersey so that each system registry will synchronize with and between the 2 states. Connecticut and Puerto Rico appear to be interested in linking into the New Jersey/New York network. The New Jersey team has completed preliminary exchange of data with New York City and has already observed gaps in both states' immunization registries. This finding confirms the need for private and secure exchange of information to ensure that children receive optimal care and all required vaccinations.

#### **4.1.21 New Mexico**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In October 2004, the Lovelace Clinic Foundation (LCF), the primary subcontractor for the New Mexico Department of Health, was awarded a 3-year grant by AHRQ to create the New Mexico Health Information Collaborative (NMHIC), a communitywide health information exchange. At the time the Privacy and Security Solutions project proposal was written, NMHIC had already accomplished the following: (1) formed a statewide steering committee with representatives from 25 health care and community organizations; (2) made significant progress in the development of software to operate an HIE, including a master patient index; (3) entered into agreements with 9 health care organizations for the sharing of data with NMHIC to develop and test the master patient index; and (4) circulated for comment legal agreements for participation in the NMHIC HIE. During these activities, the NMHIC team worked with its steering committee's organizations to identify and resolve privacy and security barriers that interfere with sharing data in a communitywide HIE.

On a parallel path, the New Mexico Medical Review Association (NMMRA) started working in late 2004 to serve as CMS's arm in the state working directly with physician office practices to promote the adoption of EHR systems as part of the DOQ-IT program. In this capacity, NMMRA developed, adapted, and employed educational materials to assist physicians in undertaking needs assessments, making the business case for converting to an electronic record system, asking the right questions of potential vendors, and identifying potential changes in office workflow redesign.

LCF and NMMRA spearheaded a collaborative effort to bring together on a systematic basis the organizations that were leaders in the state in various areas of health IT. These groups had previously proceeded with little or no coordination. Before long, the focus shifted to working to establish a New Mexico RHIO. The New Mexico RHIO development coalition includes the following:

- New Mexico Health Information Collaborative (developing the HIE)
- New Mexico Telehealth Alliance (running a statewide telehealth network)
- New Mexico Medical Review Association (CMS-designated Quality Improvement Organization for New Mexico)
- New Mexico Coalition of Health Information Leadership Initiatives (a forum to provide education for health IT)
- New Mexico Medical Society (state professional organization for physicians)
- New Mexico Department of Health (developer of numerous state registries)

As one of its initial activities, the New Mexico RHIO coalition identified and surveyed a wide range of organizations to determine specific existing health IT capabilities, services, and

future plans. This scan indicated that many organizations in the state were involved in various health IT initiatives.

### *Current Health IT/HIE Landscape*

LCF received one of the contracts totaling \$22.5 million that have been awarded to 9 HIEs to begin NHIN trial implementations.

The New Mexico Medicaid program has connected with the pharmacy network, Affiliated Computer Services, Inc, and RxHub, which are joining to provide an e-prescribing network infrastructure that will allow physicians access to New Mexico Medicaid recipients' drug histories to make more informed prescribing decisions.

For the past 3 years, New Mexico, through various projects, has been engaged in the development of an HIE network. Before the Privacy and Security Solutions project, New Mexico was already involved in building the initial community governance structure and technical architecture for the state HIE through AHRQ support, matching community funds, and funding from the state legislature. In addition to the Privacy and Security Solutions project awards (which funded related work), New Mexico submitted 2 large proposals for federal health information exchange contracts: (1) a proposal was submitted by LCF to CDC (in conjunction with the Department of Health) for accelerating situational awareness through health information exchange (biosurveillance) and (2) a proposal submitted by LCF to ONC to participate in an NHIN trial implementation. The Privacy and Security Solutions project also helped to bring the stakeholder groups together and get them actively engaged in this issue, thereby creating a greater awareness of the need for a consistent approach to ensuring privacy and security of health care information in electronic form.

### *Current Privacy and Security Landscape*

The most tangible outcome of the Privacy and Security Solutions project thus far is an effort to create and pass new state privacy legislation addressing EHRs and electronic health information exchange in the 2008 state legislative session. The need for this privacy legislation came directly from the work group meetings in the first phase of the project. The project identified widespread misunderstanding of key aspects of HIPAA leading to variations in the application of the HIPAA Rule.

The objective of the new legislation in New Mexico is a balance of the desire of patients to control access to their personal health data versus the desire of providers, payers, and health information exchange stakeholders to avoid disruptive consent process changes, associated time and expense, and delays in realizing the benefits of efficient exchange of electronic health information across organizations. The New Mexico draft legislation borrowed from similar legislation proposed in Minnesota (see discussion under that section).

Plans for project continuation through year end and beyond include: continue to solicit input about the legislation from stakeholder groups; introduce a final revised version of the bill during the 2008 Legislative Session; if legislation is passed, meet with stakeholder groups of all types to educate them concerning key bill components and identify the most efficient methods of compliance; or, if the bill is not passed, brainstorm with legislators and other stakeholders concerning issues and next steps; and introduce the revised bill in the 2009 session.

The Privacy and Security Solutions project engaged and educated a large number of stakeholders on privacy, security, and other issues about development of a statewide HIE for New Mexico. It led to greater awareness of the need for a consistent approach to ensuring the privacy and security of health care information in electronic form.

A significant contribution of the project is an elevated awareness of health information exchange issues and their importance. The Privacy and Security Solutions project has further engaged the governor's Telehealth and Health Information Technology Commission on privacy issues in general, as well as drawing its attention to health information exchange. The governor has decided to incorporate the proposed new privacy legislation in his major initiative to expand coverage to the uninsured and also to develop a plan that would require providers to develop EHR capability and exchange data through the statewide HIE.

As a result of the project, New Mexico health information exchange leaders have identified and contacted stakeholders that might not otherwise have become involved, through a range of interactions including discussions with state agencies, community forums, and town hall-type meetings. The Telehealth and Health Information Technology Commission is a formal governance structure for privacy and security created by New Mexico statute to serve in this capacity.

#### **4.1.22 New York**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

At the time the Privacy and Security Solutions project was initiated, a number of health information exchange initiatives had been started in New York, focused on improving connectivity, establishing a common governance, and integrating technology. State and local government initiatives directly supported the creation of health information exchange collaboratives, as well as other private initiatives that considered the involvement of health information exchange to be an important emerging policy. These initiatives include the following:

- **Health Care Efficiency and Affordability Law for New Yorkers (HEAL-NY).** To address a mounting financial crisis among New York's hospitals, the state passed

legislation in 2004 establishing a \$1 billion capital grants program to support the restructuring of New York's hospital systems through appropriate closures, conversions, and consolidations, as well as investment in health IT. HEAL Phase 1 awarded almost \$53 million to fund 26 HIE projects in New York State. The funding level was \$105.75 million for HEAL Phase 5, which is focusing on RHIOs and communitywide health IT adoption.

- **Health Information Technology Work Group.** In early 2005, the New York State Department of Health (NYSDOH) established this work group with representation from all departments and divisions of NYSDOH and all other state departments and agencies affected by health IT; its goal is to provide recommendations on policy positions.
- **Health IT Website.** NYSDOH launched a health IT website in March 2006 as part of the department's existing site. The website has been designed to educate participants and consumers in various health IT initiatives across the state, including the Privacy and Security Solutions project.
- **Private Grant Opportunities.** NYSDOH developed a 68-page list of private grant opportunities for parties interested in health IT. The list was published on the NYSDOH health IT website.
- **Pay-for-Performance Demonstration Project.** The 2005 state budget created a new pay-for-performance demonstration project to promote patient safety, quality of care, and cost effectiveness.
- **Health Information Technology Demonstration Project.** Passed into law in 2005, this project authorized the commissioner to issue grants for research and demonstration projects designed to promote the development of technology that would facilitate the adoption of interoperable health records.
- **Telemedicine Demonstration Project.** The 2005 state budget provided funding for a telemedicine demonstration program. The program supports research and telemedicine projects to improve the quality of home care services.
- **New York City Health IT Initiative.** New York City will invest \$25 million to provide EMRs and e-prescribing systems to physicians who care for the poorest and sickest patients. The program's goal is to reduce disparities by creating EHRs at community centers, allowing them to interface with systems in place at public hospitals and clinics.
- **NHIN Trial Implementations.** The New York eHealth Collaborative was one of 9 organizations participating in the NHIN Trial Implementations.

In addition to statewide health IT initiatives, a number of private-sector health IT initiatives existed in New York, including several RHIOs. Each varied in its levels of implementation, and most assembled a broad group of health care stakeholders to assist with the initiative. For example, in January 2005, the New York State Health Information Technology Summit brought together private- and public-sector leaders to discuss the role of health IT in the evolving health care marketplace and to develop a public policy framework to advance health information exchange in New York State. Shortly after the summit, the state issued a request for proposal for the first round of financing through HEAL-NY. The state received

more than 100 requests for funding for health information exchange projects. Following are examples of health information exchange projects in New York State as of February 2006:

- New York Clinical Information Exchange—a data exchange to deploy continuity of care record-type data elements to emergency department clinicians.
- Upper Manhattan Health Initiative, Northern Manhattan—data communication capabilities to create patient registries for chronic conditions, to define and implement data standards, and identify and adopt chronic care standards of care.
- Health Connection Card Program, Queens—portable, accessible personal health record on a smart card. The plan is to expand this project to create an electronic data exchange to enable hospitals, physician practices, health plans, mental health providers, labs, pharmacies, and home care agencies to access real-time patient data.
- Brooklyn HIE—electronic data exchange among participating organizations focused on disease management across the continuum of care for persons with complex, chronic diseases.
- Bronx RHIO—data exchange among participating organizations for a core minimum data set, including lab and pharmacy information, hospital and ED discharge diagnosis, imaging study reports, allergy information, and other key data.
- New York Community Home Health Care Interoperability Project—electronic data exchange to enable physicians and home care clinicians to update and exchange data from their own EMR.
- Long Island Patient Information Exchange—a RHIO on Long Island for patient clinical information sharing.
- Healing NY with Health e-Technology, Long Island—a RHIO in Suffolk County for clinical data sharing, e-prescribing, and EMR access.
- Taconic Health Information Network and Community, Hudson Valley—a community health care portal that integrates existing electronic messaging and clinical data exchange with a full EMR for the majority of health care providers in Dutchess, Ulster, and Putnam Counties.
- Greater Hudson Valley Regional Health Information Organization—a centralized clinical database repository and a clinical information data exchange among participating providers.
- Adirondack Medical Center, Saranac Lake—a network of shared information among the area's only acute care hospital, 9 physician practices, 4 clinics, and the major payer in the area.
- Health Information Exchange of New York, Capital District—clinical information data exchange to improve quality, efficiency, and safety of the health care system by making prescription medication information available electronically at the point of care.
- Adirondack Health Information Exchange, Southern Adirondacks—portal to exchange clinical data with results reporting, e-prescribing, patient education, and secure physician/patient functionality.

- Southern Tier HealthLink, Binghamton and Surrounding Counties—regional portal to give clinicians access to real-time electronic patient records, expand the HIE interoperability infrastructure, develop EMRs, and connect necessary organizations.
- Rochester Regional Health Information Organization—an IT database and application integration hub to accelerate the exchange of patient data across 9 counties of the greater Rochester area.
- Western NY Clinical Information Exchange, Buffalo Area—an online community health network for clinical data exchange, a data repository, e-prescribing, and a diagnostic data network.

### *Current Health IT/HIE Landscape*

New York State is engaged in a statewide strategy to promote improvements in health care quality, affordability, and outcomes through the widespread adoption of health information technology. The state has secured and made available significant financial resources, established executive-level health IT policy leadership with a new health IT office, and designated a statewide public-private partnership to facilitate a collaboration process with an open and transparent dialogue to lay the foundation for development of New York's health information infrastructure. In addition, New York has promoted the development of public-private partnerships that provide strategic development, technical assistance, and evaluation for emerging health information exchange projects.

On April 9, 2007, the NYSDOH commissioner announced the creation of an Office of Health Information Technology Transformation (OHITT). OHITT will be responsible for leading state and private-sector efforts to improve health care quality, accountability, and efficiency through widespread deployment of health IT.

Additionally, OHITT will have primary responsibility for coordinating the state's substantial funding for health IT projects under the HEAL-NY Capital Grant Program, and the evaluation of those projects in collaboration with the academic consortium known as the Health Information Technology Evaluation Collaborative. OHITT will also collaborate with the state Medicaid program and other NYSDOH programs on a variety of health IT initiatives. The work of the New York team will have an impact on HEAL grantees as they implement their projects.

The project team in New York identified several key project outcomes related to general health IT and electronic health information exchange. Specifically, the team convened stakeholders to identify issues about implementation of privacy policies that will support interoperable exchange. The work performed in the Privacy and Security Solutions project is also being used by HEAL grantees as they work toward implementation. In addition, the consensus-building process is working, and the team noted that they are much closer to consensus than they were several months ago. The high levels of interest in participation among stakeholders have contributed to this success.

The New York eHealth Collaborative is organized to include privacy and security in the overall governance structure but is not specifically dedicated to privacy and security. RHIOs have their own policies, and the team is working to include privacy and security requirements in future state and HEAL grants.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project is integral to advancing the state's health information exchange activities. Through the first phase of the project, the New York team identified 4 priority solution areas that support the privacy and security of electronic exchange of health information: patient engagement, consent, security/access/use, and patient identification. For the second phase, the New York project team is developing solutions to patient consent issues and an implementation plan for RHIOs. In the first phase, the project team learned that RHIOs across New York State have an urgent need for guidance on obtaining adequate and meaningful patient consent. In the absence of such guidance, RHIOs and other health information exchange projects have been left to develop their own policies that govern consent to exchange patient health information. As a result, health information exchange projects have been taking disparate approaches, often based on varying interpretations of existing state law and public policy priorities.

The project team facilitated 3 stakeholder meetings on this topic in September and October, 2 in New York City and one in Albany. More than 60 people attended each meeting, including consumer advocates, RHIO administrative and clinical leadership, New York City Department of Health and Mental Hygiene representatives, health plan representatives, and lawyers, among others. The first meeting was dedicated to understanding the current state of RHIO policy development regarding consent in New York. The second meeting sought to elicit discussion on the key policy questions that a new consent policy for RHIOs would need to address. At the third meeting, "straw model" patient consent policies and procedures were proposed and discussed.

The discussion at the 3 meetings has led to the development of a statewide consumer consent policy and process published in a policy white paper. The purpose of the white paper is to put forth recommended policies and guidelines for public comment. The policies and guidelines would govern consumer consent for the exchange of personal health information facilitated by RHIOs. The goal of the recommendations is to protect privacy and strengthen security in a technology-enabled health care environment. The white paper will be posted on the NYSDOH website, with an invitation for all stakeholders in New York to submit comments. Comments received will be reviewed and considered during the development of final policy guidance that will be issued by the NYSDOH.

After reviewing the comments submitted in response to the policy white paper, the NYSDOH will issue final policy guidance and take action to include its recommendations in all future contracts with RHIOs in New York. The contract provisions will require RHIOs to:

- Adopt privacy policies and procedures consistent with state recommendations;
- Use the standardized RHIO consent form approved by New York State; and
- Participate in a consumer education program initiative launched through the statewide collaboration process to support the privacy policies and procedures.

The team recognizes that further work and ongoing guidance is necessary to ensure the successful implementation of patient consent policies and procedures proposed in the policy white paper. The implementation of the policies and procedures will be facilitated by the New York eHealth Collaborative (NYeC), a public-private partnership, to advance health IT initiatives in New York. The New York team has identified the following issues that will require attention through a statewide collaboration process:

- a more precise definition of “one-to-one” health information exchange;
- development of consumer education materials and campaign;
- consent policies and procedures for use of de-identified data exchanged through RHIOs, focusing on ensuring adequate protections against re-identification;
- consent policies and procedures relating to minors;
- consent policies and procedures relating to information obtained from federally qualified substance abuse facilities; and
- development of a cohesive state regulatory solution for health information exchange, such as accreditation of entities governing health information exchange initiatives (ie, RHIOs).

As the New York project team facilitated stakeholder meetings, it became clear that implementing the state’s priorities regarding patient consent policies through contractual relationships at this point, instead of legislation, is a more effective means of implementation. It is anticipated that legislation will be introduced in the future, but the project team concluded that development of legislation during the project period would be premature.

The Privacy and Security Solutions project has had a significant impact on HEAL projects by encouraging a concentration on policy development to implement interoperable health information exchange. At the time of original funding, HEAL projects were not attuned to this area, but now, because of the Privacy and Security Solutions project, they have been engaged in the process and realize the importance and need for developing their privacy policies. A significant impact of the Privacy and Security Solutions project has been to bring stakeholders together to identify issues involved with implementation of privacy policies for interoperable exchanges. HEAL grantees are using and building on the Privacy and Security Solutions project work as they work toward implementation of these policies. A portion of the funding for the HEAL grantees will be used to continue the work of the New York Privacy and Security Solutions project.

The project has also led the team to identify or interact with stakeholders that they might not otherwise have worked with, particularly individual consumers and consumer advocacy groups. The Privacy and Security Solutions project compelled the team to address consumer engagement sooner rather than later. The team has also worked with the Office of Mental Health, the Office of Mental Retardation and Developmental Disabilities, the State Insurance Department, and the Attorney General's Office. The team stated that this communication would have happened eventually, but the Privacy and Security Solutions project gave them the chance to engage earlier and in greater depth.

The Privacy and Security Solutions project has encouraged collaboration with other states in implementing privacy and security solutions that will work across state boundaries. New York is working with New Jersey to implement a system for electronic exchange of immunization registry information. Participation in collaborative work groups for consent and consumer engagement is also continuing on the national front. The Privacy and Security Solutions project has supported work to advance privacy and security throughout the state.

#### **4.1.23 North Carolina**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

The North Carolina Healthcare Information and Communication Alliance (NCHICA—the governor's designee for the Privacy and Security Solutions project) was established by executive order of the governor in 1994 to improve health and care in North Carolina by accelerating the adoption of information technology. Since then, NCHICA has led efforts in developing model privacy legislation (1995–1999), developed tools for HIPAA compliance (1999–2003), and facilitated initiatives to demonstrate the secure exchange of health information on a statewide basis (1998–2005).

Several health IT initiatives were under way in North Carolina at the time the Privacy and Security Solutions project began. The NCHICA Board's 2003 vision of the North Carolina Healthcare Quality Initiative articulated the need for a multiple-stakeholder project designed to automate medication, laboratory, and radiology data. The first phase of this project involved providing a list of patient medications to the patient's health care provider at the point of contact so the provider can evaluate possible drug-to-drug interactions and prescribe correct dosages. The electronic information would be accessible by providers, health plans, pharmacy benefits managers, and pharmacies. The second phase of the project involved the electronic exchange of lab and radiology data to further improve care and save time. This vision has guided and encouraged NCHICA to seek out demonstration projects that would realize this goal over a number of years.

Independently developed by Duke University, the Automated Adverse Drug Events Detection and Intervention project established an automated surveillance system for

detecting, reporting, intervening in, and measuring the incidence and nature of adverse drug events suffered by patients. The system is designed to alert physicians about critical detected events, and certain triggers will result in automated reports that will be evaluated on a daily basis by pharmacists trained in adverse drug event investigation.

The North Carolina Emergency Department Database (NCEDD) project began in 1999 as a collaborative effort between CDC, the North Carolina Division of Public Health, the University of North Carolina-Chapel Hill Department of Emergency Medicine, the North Carolina College of Emergency Physicians, and NCHICA. The initiative created an emergency department data repository for the North Carolina Division of Public Health. NCEDD collected, standardized, and analyzed timely and secure emergency department clinical and administrative data. It led to the 2005 launch of the North Carolina Hospital Emergency Surveillance System (NCHES), a mandated emergency department collection system that is expected to assist the state in the early detection of and response to public health emergencies or potential biological or chemical terrorist attacks. A related project is the North Carolina Disease Event Tracking and Epidemiologic Collection Tool (NC DETECT), an early event detection system allowing authorized users to view data from NCEDD and the Carolinas Poison Center, North Carolina Wildlife Center, and other data sources for a variety of public health surveillance needs. Over 5000 emergency room visits per day are reported to NCHES electronically in near real time. Early in the initiation phase of NCEDD, the NCHICA Board of Directors designated NCEDD as an “exemplar project” and assigned a special task force to ensure that all aspects of the HIPAA Privacy and Security Rules were taken into consideration in the development of policies and procedures for the project.

The University of North Carolina Hospital System implemented a Perinatal EMR project, involving an electronic version of prenatal medical records integrated into software to facilitate the input, storage, retrieval, and modification of prenatal records. The software was designed to allow patient access to medical data through a wireless LAN. The data can be transferred to and from a centralized database and can be shared with others over the Internet for clinical and research purposes.

Another initiative focusing on children’s health care was the Provider Access to Immunization Registry Securely (PAIRS) system. Started in 1998 as a collaborative effort among the North Carolina Division of Public Health, Blue Cross Blue Shield, Kaiser-Permanente Foundation, Initiate Systems, Quintiles Transnational, EDS, and the North Carolina Pediatric Society, PAIRS was an early, critical component in North Carolina’s development of a statewide immunization registry, which was implemented in 2005. PAIRS used probabilistic matching to identify records from disparate databases that belonged to the same patient. North Carolina gained valuable early experience with the crucial element of matching records without a unique patient identifier.

NCHICA collaborated with IBM under the NHIN Phase I contract with ONC to develop the prototype architecture for the NHIN. Communities in Research Triangle Park, NC, Guilford and Rockingham counties, NC, and Danville, VA, participated with NCHICA in this prototype work.

In the private sector, various health care stakeholders participated in regional and community HIEs. The Western North Carolina Health Network, a consortium of 16 hospitals in the Blue Ridge Mountains, was one of the first regionwide HIEs in North Carolina. The participants can view patient data from each of the other participating hospitals through a virtual EMR system, and each authorized user has a standardized view of the data.

### *Current Health IT/HIE Landscape*

NCHICA is also involved in federal efforts such as the Health Information Protection Task Force of the NGA State Alliance for e-Health, Health Information Technology Standards Panel (HITSP), and the Certification Commission for Healthcare Information Technology (CCHIT), which has helped the overall ability for electronic health information exchange to succeed in North Carolina. NCHICA is a US Department of Health and Human Services “Community Leader” in “Value-driven Healthcare” through Secretary Leavitt and AHRQ. A Community Leader is a multiorganization collaborative (mostly nonprofits in health care) that addresses the 4 cornerstones of the project. The collaborative is eligible to become a “Chartered Value Exchange” that collects and publishes quality and price data.

NCHICA is also one of 9 organizations awarded a contract for the NHIN trial implementations. Necessitated by the NHIN trial implementation proposal, NCHICA created the North Carolina Health Information Exchange Governance Council to provide a multisector, statewide body to work on policies and procedures, security infrastructure, and business practices to allow secure exchange of health data to improve the quality and value of care given in North Carolina.

One of North Carolina’s goals throughout the Privacy and Security Solutions project was to build leadership and gain executive-level private and public sponsorship through awareness and outreach programs. To achieve this goal, project team members in North Carolina developed, presented, attended, and hosted numerous informational programs to raise awareness of current health information exchange initiatives underway and the effects these exchanges have on privacy and security considerations for the consumers, employers, legal community, and public policy makers. Through these meetings, presentations, and participation in the National Governor’s Association State Alliance for e-Health, North Carolina has extended its communication efforts beyond its NCHICA membership by opening a new dialog with consumers, public policy makers in North Carolina’s State House and Senate, the North Carolina Medical Society, the North Carolina Hospital Association, and the governor’s office.

### *Current Privacy and Security Landscape*

Through the Privacy and Security Solutions project, NCHICA engaged consumers by creating the Consumer Advisory Council on Health Information (CACHI). CACHI members are instrumental in vetting educational tools aimed at consumers and bringing consumers' point of view to the table during discussions about health IT and health information exchange. In addition to consumer involvement, this project has allowed NCHICA to create materials aimed at educating legislators and providers. CACHI helped the North Carolina project team with several projects throughout both phases of the Privacy and Security Solutions project. Activities included

- developing a long-term strategy and process that will act as a road map the Council can use to address privacy and security concerns; and
- developing a program to raise broader consumer and provider awareness for the general public on issues surrounding health information privacy and the risks and benefits of health IT.

Another goal of the North Carolina project team was to reduce legal barriers to timely health information exchange. The initial phase of the strategy was to raise awareness about the foundational work conducted by the project's LWG. This group reviewed the NC HIPAA Preemption Analysis to identify potential barriers to health information exchange and to identify all consent related statutes. The LWG also prepared a draft model patient consent form and data exchange agreements to be used by organizations engaging in health information exchange. As a result of the work conducted in the Privacy and Security Solutions project, stakeholders were given an opportunity to focus solely on the business practices, policy, and legal drivers that create barriers to the secure and timely exchange of health information.

The Privacy and Security Solutions project has accelerated and further cemented the ongoing process for formulation and implementation of interstate privacy and security policies for health information exchange. Since 1995, the state has had a Privacy and Confidentiality Work Group (now called the HIPAA Privacy and Security Officials Work Group) in place to scan federal and state laws to see if they could build model privacy laws or policies to fit the national and state needs to protect health information. The Privacy and Security Solutions project is working closely with this work group to accelerate its activities.

The Privacy and Security Solutions project also encouraged North Carolina health care stakeholders to work with other states to formulate and implement privacy and security solutions. Collaborating and exchanging ideas with their counterparts has proven to be one of the most effective means for NCHICA to gain the interest and involvement of the health care community. With the emphasis on privacy and security policy, law, and regulation, the project has given North Carolina the opportunity to update work previously conducted by various privacy and security work groups. Most importantly, a dialog has been created among professional health care stakeholders, public policy makers, and consumers.

#### **4.1.24 Ohio**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Since 2002, Ohio's Third Frontier Project, a publicly funded effort to promote information technology in the state, has invested more than \$207 million in 15 biomedical public-private commercialization partnerships, ranging from cardiovascular, cancer, and neuromodulation to imaging, stem cells, and bioinformatics.

In October 2005, the Health Policy Institute of Ohio (HPIO) published *Assessing Health Information Technology in Ohio: Briefing Paper for the 2005 Health Information Symposium*. This monograph reported on electronic records in 13 hospitals and several hospital systems, many using computerized physician order entry (CPOE). Many more hospitals and hospital systems were implementing enterprise solutions for health IT in their organizations. Three health IT research projects involving e-prescribing and disease management programs had been funded, 2 by AHRQ and 1 by an Ohio philanthropic organization.

##### *Current Health IT/HIE Landscape*

Several health IT/health information exchange efforts have been initiated at the local level in Ohio. The infrastructure for the Community Health Alliance of Northwest Ohio (Toledo) includes a community-centric data processing center and a highly leveraged service center. Key components of the system are the consistent identification of each patient across institutional boundaries and the automatic distribution of information between care sites according to privacy-protected routing rules.

Many groups in the northeastern area of Ohio (Cleveland, Akron, Canton, and Youngstown) are engaged in activities to promote the effective adoption of health IT and health information exchange. This work includes individual projects aimed at promoting greater use among long-term care facilities, small physician practices, federally qualified health centers, and the region's major hospitals. In addition, several Cleveland hospitals were part of the third community of NHIN awardees to develop prototype architectures, led by Northrop Grumman. In 2006, the Northeast Ohio Regional Health Information Organization was created in the Cleveland-Akron area.

In Central Ohio, 3 major health systems—The Ohio State University Medical Center, Ohio Health, and Mt. Carmel Health System—along with Select Specialty Hospitals have a Clinical Work Group that is developing a clinical transaction based on the continuity of care record concept. The initial stages of the project will focus on the transfer of demographic and clinical data on patients being referred from one of the health systems to a Select Specialty facility.

In Dayton, the Center for Health Communities, a division of Wright State University Boonshoft School of Medicine, has implemented a shared, communitywide health record based on the Community of Care Record standard. The web-based data system, called HIE<sup>™</sup>, now houses patient and household-centric demographic and health data on 20000 individuals.

HealthBridge, located in Cincinnati, is an Internet portal used by more than 100 health entities and thousands of providers. Providers retrieve clinical information in a standardized format, developed through the collaboration of members. This HIE has several critical components, including secure connections between physician organizations and hospitals, access to existing hospital information, and a communitywide clinical messaging system. Data from multiple sources are standardized across the community and delivered electronically to physicians.

In the heavily rural southeastern part of the state, the Appalachian Regional Informatics Consortium (ARIC) has been funded by the National Library of Medicine. The consortium's mission is to create a sustainable and replicable model for advanced integrated information management systems for rural health care in the Appalachian counties of Ohio.

The HPIO, Wright State University Center for Healthy Communities, and Ohio KePRO have cosponsored statewide health IT events from 2004 to 2007, bringing together a variety of stakeholders to discuss health IT and health information exchange projects.

In October 2007, Governor Strickland issued an order to create an advisory board to coordinate public and private efforts aimed at fostering statewide health information exchange efforts. The Ohio Health Information Partnership Advisory Board is chaired by the state's chief information officer and has the task of developing a plan for coordinating health information exchange. The board will help to coordinate all Ohio health information exchange efforts. The group has just over 12 months to develop the plans.

OhioHealth, a health system including 15 hospitals, 20 health and surgery centers, home health, and durable medical equipment services, has implemented an e-prescribing application for its 2300 physicians. The technology allows physicians to both transmit prescriptions and receive messages back from pharmacies, including electronic refill requests.

Ohio has also been collaborating across states in formulating and implementing privacy and security solutions with Kentucky, Michigan, Minnesota, New Jersey, Pennsylvania, and West Virginia. Ohio is working with Kentucky and West Virginia on permission forms, because these states have expressed interest in the Ohio form and perhaps adapting or adopting it as a common form for interstate exchange of information.

### *Current Privacy and Security Landscape*

The first phase of Ohio's Privacy and Security Solutions project identified significant legal barriers to health information exchange in the areas of patient permission to exchange information and the lack of standards for role-based access to patient data. Throughout Phase I of the project, the HPIO was able to elevate the discussion related to privacy and security through the various project work groups and community forums. In addition, the HPIO proved to be a key facilitator in bringing various stakeholder groups together to identify how security and privacy concerns could be addressed as the state moves forward with health information exchange. As a result, the landscape in Ohio with respect to privacy and security has been dramatically improved and has positioned the state to move forward with state-wide exchange between the existing and developing RHIO organizations.

In Phase II, Ohio implemented 2 distinct projects, a model permission form project and a role-based access project. The model permission form project used the LWG as the development team for a universal permission form. The LWG comprised broad-based stakeholder representatives from numerous health interests to help ensure a comprehensive review of state and federal laws regarding the use and disclosure of patient information. The group addressed the issue of inconsistent interpretation of consent requirements for treatment, payment, and operations. They also reduced confusion and enhanced readability of the form by separating 2 sections of a single form into 2 distinct forms. This project produced the state of Ohio patient permission forms, which comply with all legal requirements in the state. They anticipate that the forms will be approved by the project steering committee in December 2007.

The role-based access project involved substantial research into how other states were addressing the issue of access in an attempt to standardize an approach expandable to other states. This group used the concepts of authorization, authentication, access control and audit, and adapted them to make specific recommendations appropriate for Ohio. This group completed their strategy document in November 2007 with final review and approval by the steering committee expected in December 2007.

In October 2007, HPIO formed the consumer education work group, representing a wide range of consumer advocacy groups and associations. This group is responsible for informing consumers of the value of electronic exchange to help alleviate consumer fears related to data privacy and security.

Also in October 2007, Governor Strickland signed an executive order creating the Ohio Health Information Partnership (OHIP) Advisory Board. The Board has a broad-based composition of consumers, providers, employers, government, and health plans. Their mission is to bring together broad-based private and public sector representatives to formulate policies and programs that address health information technology and exchange issues in Ohio. The governor has emphasized the importance of ensuring that all data

exchange be conducted in accordance with nationally accepted standards of privacy and security. The executive order lays the groundwork for voluntary implementation in 2008 of the permission forms created by Ohio's Privacy and Security Solutions project. In addition, the project team has successfully engaged state government, RHIOs, consumers, employers, providers, and payers in discussions that will lead to the creation of a statewide health information exchange.

To facilitate effective exchange of health information and improve health care quality, Ohio has focused stakeholder discussion on privacy and security barriers to health information exchange, potential solutions, and best practices. Several federal- and state-sponsored initiatives are working toward a smooth transition from paper-based records to electronic data exchange. The governor's executive order to establish a quasi-governmental public/private oversight collaborative body is a first step toward establishing a governance structure for health IT (Executive Order 30S, September 17, 2007). Privacy and security initiatives being addressed by the Privacy and Security Solutions project will constitute an important part of that body's agenda. One of the major impacts of the project has been to facilitate and accelerate interstate activities for implementation and formulation of privacy and security policies. Ohio is working closely with Kentucky, Michigan, Minnesota, New Jersey, Pennsylvania, and West Virginia on issues such as consent forms and related topics.

#### **4.1.25 Oklahoma**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Prior to the Privacy and Security Solutions project, Oklahoma had developed some history with electronic health information exchange. On November 17, 2005, the Oklahoma Hospital Association and the National Alliance for Health Information Technology hosted a meeting on health care stakeholders in Oklahoma to provide education and begin to gauge interest in establishing a statewide health care data and information exchange. A health information exchange professional was consulted to help identify key health care stakeholders and assess expectations and concerns about forming statewide, regional, or provider/integrated health system–centric HIEs and RHIOs.

Oklahoma had 5 sites that use the Indian Health Service Electronic Health Record geographical user interface for patient care: Carnegie Health Center, W. W. Hastings Indian Hospital in Tahlequah, Carl Albert Indian Hospital in Ada, Purcell Health Clinic, and Claremore Indian Hospital.

The Healthy Community Access Program was also established as a collaborative effort of the Tulsa Health Department and Community HealthNet. It featured CareLink, a system to increase access for the uninsured, underinsured, and Medicaid eligible. The CareLink umbrella included NurseLink, a telephone medical advice triage system, and HealthLink, a

telephone appointment system. CareLink was also a member of ShareLink, a client referral system for community health networks, that helps local health programs and agencies provide a continuum of care.

SMRTNET, formerly the Health Improvement Collaboration in Cherokee County, was a coalition of several state, federal, and local agencies in Oklahoma that was awarded a grant by AHRQ to build an interoperable electronic health care system between the provider agencies. It was the first demonstration project of interoperable electronic health information exchange in Oklahoma. The Cherokee County Health Improvement Collaboration had 3 primary outcomes: (1) an integrated, multifunctional, HIPAA-compliant community health information network that enabled providers to coordinate care and facilitate client access to a wide range of medical services; (2) a telephonic comprehensive nurse line service and triage function to provide appropriate interaction with patients, improve overall quality care, and reduce inappropriate use of hospital emergency rooms for nonemergent care; and (3) implement improvements in existing appointment systems.

The Oklahoma Foundation for Medical Quality (OFMQ) was designated as the Medicare Quality Improvement Organization for the state and was involved with the DOQ-IT project. DOQ-IT helped primary care practices understand and use health IT. OFMQ offered support to practices implementing clinical information technology solutions or improving efficiencies of current systems, such as a full EHR or a registry system (for tracking patients with chronic diseases), along with e-prescribing.

Saint Francis Heart Hospital had laid the technical foundation for an HIE. The cardiovascular network included outpatient diagnostic centers, ambulatory clinics, tertiary care centers, and independent physician practices. This safety network captured historical data for cardiovascular-comprised patients, with the objective of affecting outcomes in a positive manner by eliminating paper-based problems.

INTEGRIS Telewound Network was underway to demonstrate and evaluate the clinical effectiveness and cost savings of using telehealth technology to reduce the number of days of healing for chronic wounds by improving access to caregivers, point-of-care services, and dissemination of best practice information.

The Oklahoma State and Education Employees Group Insurance Board (OSEEGIB) was the primary provider of health benefits for state, education, and local government employees and retirees of the State of Oklahoma. The board developed processes for exchanging eligibility information, claim information, and payment information with 22 different business partners, including other state agencies, third-party administrators, and health maintenance organizations. These data exchanges were responsible for approximately 460 file transfers per month, with frequencies ranging from daily to annually. The coordination of electronic health information between OSEEGIB and its business partners was seen as

necessary to maintain eligibility integrity between many databases, ensuring the proper level of coverage and ultimately the accurate processing of claims.

### *Current Health IT/HIE Landscape*

Electronic health information exchange is in the early stages in Oklahoma, but it is growing rapidly. Overly restrictive interpretations of HIPAA, other privacy and security concerns, and expense are major barriers to the expansion of health IT and health information exchange. Many entities have business practices in place that are more restrictive than state and federal privacy and security law requires. This conservative approach was found to be based primarily on a lack of understanding or misinterpretation of laws and regulations governing the release of personal health information.

Oklahoma continues to build on the solid foundation for interoperable exchange for the future. It is anticipated that the governor's office will issue an executive order to keep the Privacy and Security Solutions steering committee intact. The goal is not only to continue work, but also to be the coordinating body for all health information exchange efforts around the state.

Recent health IT/health information exchange activity in Oklahoma includes the following:

- The emergency department at Jane Phillips Medical Center in Oklahoma has deployed Cerner FirstNet, a clinical information computer system that will allow clinical staff to create a complete EMR of patients they see in the emergency department.
- Comanche County Memorial Hospital, a 283-bed facility in Lawton, will spend about \$13 million in efforts to go paperless and boost patient safety. The hospital recently selected a wide range of technology developed by McKesson Corporation. The goal is to create a single, secure EHR flowing across hospital departments and local physician offices. Under terms of the multiphase initiative, the hospital will deploy a combination of the Horizon Clinicals suite, along with resource management systems and information technology services.
- Oklahoma has 13 FQHCs with 25 sites. Of these 13, more than half have adopted EMRs. FQHCs have largely developed their systems independently of each other; however, 2 recently funded FQHCs have collaborated with centers to adopt existing systems that would eventually provide interoperability between the new centers and their collaborative partners. Statewide, FQHCs are pursuing HRSA data and quality initiatives that encourage and support the adoption of electronic health information exchange.

### *Current Privacy and Security Landscape*

One of the major recommendations to emerge from Phase I of the Privacy and Security Solutions project was the need to create an Office of Health Information Exchange (OHIE). During Phase II, efforts were focused on establishing recommendations for a framework and structure for privacy and security issues for the OHIE. The Oklahoma project's steering committee recommended that the OHIE should be an office under the Office of the

Secretary of Health, with an external board of directors and advisory committee. The steering committee also developed the mission, vision, and values for OHIE. The project team held 2 WebEx conferences to collect input on the functions and structure of OHIE from consumers and stakeholders throughout the state.

The OHIE will be entrusted with becoming a statewide resource for information about privacy and security issues. This recommendation was based on findings that many entities in Oklahoma had overly restrictive interpretations of HIPAA and other privacy and security laws, that very little information was being electronically exchanged, and that major concerns existed about liability for inappropriately released data.

The Oklahoma steering committee is currently working with the governor's office to develop an executive order to establish the Oklahoma Health Information Security and Privacy Council. The purpose of the Council is to continue efforts to plan and implement recommendations for the OHIE and address issues related to health IT in Oklahoma.

Another goal of the Oklahoma project team was to develop a single Authorization to Release Information form that will apply across jurisdictional lines within Oklahoma, including tribal nations and federal facilities. Findings from Phase I of the Privacy and Security Solutions project indicated that information on patient consent/release forms was not standard and different providers were using different forms.

With legal experts from the project's steering committee, personnel from the state health department developed a universal Authorization to Release Information form and a statement of compliance with state and federal statutes. Approximately 5 iterations of the form were distributed to the steering committee for input and consensus building. The fifth draft was shared among stakeholders and consumer groups in a statewide meeting to gather further input. Following the meeting, the form was posted for public comment for 2 weeks. All comments were then synthesized and integrated into the last draft. State agency attorneys and legal counsel external to Oklahoma were consulted to resolve possible issues related to compliance with Oklahoma regulations and statutes. The final draft is being prepared for the February 2008 legislative session.

The Privacy and Security Solutions project has had statewide impact on information sharing and dissemination, stakeholder knowledge, and education. The Oklahoma steering committee members have been instrumental in disseminating information about the work of the project in Oklahoma and with other states. The Oklahoma project team has also promoted the importance of public and private partnerships in facilitating health information exchange within the state.

In addition, at the most recent Summit III meeting, which is sponsored by the Oklahoma Insurance Department to identify problems and solutions in the health care system, health IT, program expansion, evidence-based practices, and children's health, 3 steering

committee members were invited to present their work. One of the goals for Summit III was to identify the top 10 priorities for the coming year. Implementing a statewide health information organization and encouraging the use of electronic medical records were ranked the top priorities by consensus.

Although Oklahoma is beginning to develop electronic health information exchange, a synergy has developed through both phases of the Privacy and Security Solutions project and the collaboration between the private and public partners. Stakeholders as varied as the leadership of the Oklahoma Health Department, the Insurance Commissioner, providers across the state, and consumers have all expressed an interest in seeing the implementation recommendations realized. In addition, a number of agencies and organizations involved in the Oklahoma project have expressed an interest in continuing to provide support to this process.

When the Privacy and Security Solutions project began, Oklahoma had several health IT/health information exchange initiatives. Some of them, such as the Secure Medical Records Transfer Network, were focused primarily on privacy and security issues related to transfer of electronic data. The Oklahoma Privacy and Security Solutions project has offered opportunities for health care professionals throughout the state to participate in identifying privacy and security practices for health information exchange. This initiative is greatly 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 major focus at the moment is on data sharing within the state. Efforts are under way to create an Office of Health Information Exchange (OHIE) that will be entrusted with becoming a statewide resource for information about privacy and security issues. Current efforts are focused on establishing a framework and structure for privacy and security issues and creating OHIE.

#### **4.1.26 Oregon**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In 2004, the Oregon Health Policy Commission formed a Subcommittee on Electronic Health Records and Data Connectivity to develop recommendations for (1) fostering the adoption of EHR in Oregon's health care delivery systems and (2) developing the infrastructure for the secure exchange of electronic health data between systems. The subcommittee report, completed in March 2005, recommended the state's role in fostering the use of interoperable EHRs. The Joint Legislative Committee on Information Management and Technology has been closely following the work of the subcommittee and has supported EHR adoption and interoperability efforts. As a result of the committee work, the Oregon

Office of Health Policy and Research has committed resources for creation of a position for health IT coordination.

The Oregon Healthcare Quality Corporation (Quality Corp) and the Oregon Business Council (OBC) have a shared long-term vision for secure health information exchange. The OBC leadership group is composed of the chief executive officers of some of the largest health systems, health plans, employers, and physician groups in the state. These leaders have committed a small amount of resources to assist Quality Corp in delineating first steps for health data exchange for Oregon. This work will facilitate completion of Quality Corp's strategic plan, which proposes a governance structure for a RHIO and incremental implementation through pilot projects.

The Oregon and Southwest Washington Healthcare Privacy and Security Forum was created in May 2000 to address Oregon's version of HIPAA compliance. The forum has been instrumental in shaping Oregon statute around privacy and security, especially during the 2003 legislative session. A comprehensive legal and statutory review was done at that time to conform state statute to federal law. The forum developed standard forms, contracts, and policies and created educational materials to assist in dispelling regulatory myths about HIPAA. It has also been active in collaborating with Alaska, Idaho, Montana, and Washington in developing privacy standards. A number of successful initiatives and work products have been produced, including an Oregon authorization form for the use or disclosure of protected health information, standard companion documents for electronic transmission of data, and privacy and security policies.

Other important privacy and security groundwork was performed by the Oregon Association of Hospitals and Health Systems, which has 2 groups: the HIPAA Security and HIPAA Privacy task forces. The Oregon Medical Association has also pioneered important groundwork as part of the Oregon Medical Electronic Network project. This effort established a statewide network that operated from 1993 to 2003 and included 12 health plans (including the state Medicaid program), several health systems, and independent physician associations for sharing eligibility data.

The Chronic Disease Data Clearinghouse project of Quality Corp, the Oregon Diabetes Coalition, and the Asthma Network also addressed policy issues for data exchange. This proof-of-concept pilot demonstrated that 12 health plans working together were able to establish and maintain data-sharing agreements. One of the products is a combined report that physicians will use to manage care for patients with diabetes and asthma.

The Oregon Health Information Infrastructure (OHII) has provided groundwork through a strategic plan, developed through stakeholder meetings. This plan proposed an agenda to encourage adoption of EHR and systems for the secure and efficient dissemination of information. OHII work has included multiple statewide conferences, forums for chief

information officers and chief medical information officers, a pilot project proposal, and an EHR inventory to establish a baseline of EHR adoption in the state.

Five groups had initiated community data exchange projects as part of the AHRQ initiative in Oregon:

- Improving the Quality of Healthcare in Central Oregon—Bend
- Bay Area Community Informatics Project—Coos Bay
- Using IT to Improve Medication Safety for Rural Elders—Lincoln City
- Medication Management: A Closed Computerized Loop—Grants Pass
- Improving Safety and Quality With Integrated Technology—Portland

### *Current Health IT/HIE Landscape*

Various initiatives are working with the state government to define boundaries for entities involved in health IT and health information exchange and to decide on a system of governance. Recent activities include the following:

- Medicaid Transformation Grant
- Electronic Health Record Implementation Initiative
- High Impact—Electronic Health Record Implementation Initiative
- Health Information Technology Innovation Initiative

A private-sector health information exchange effort in the Portland metro area is currently on hold, although some smaller rural efforts are moving forward with AHRQ funding. There is a heightened awareness of patient control issues in terms of privacy and security. A state-designated body, the Health Information Infrastructure Advisory Committee (HIIAC), is expected to create wider harmony on issues that are dividing stakeholders in the state, such as the potential for increased focus on privacy and security issues beyond HIPAA. A Health Fund Board was recently designated by the governor to oversee the HIIAC. The Health Fund Board is a higher level entity tasked with developing a plan to rebuild Oregon's health care system so it is accessible, affordable, and effective. Health IT and health information exchange will play an important role in reform measures, and privacy and security issues will garner attention as the Health Fund Board moves forward.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project helped to stimulate the creation, advancement, and endorsement of HIEs in Oregon. For example, the Health Policy Commission report devoted a section on health information exchange and privacy/security, which spurred a set of recommendations. Although the Metro Portland HIE was started before the Privacy and Security Solutions project began, the project informed the initiative about privacy and security issues.

The Oregon Health Policy Commission devoted a section of its 2007 report to the governor to privacy and security issues arising from electronic information exchange. The Commission called for state support for the implementation and dissemination of the recommendations of the Oregon project team, including the funding of a Health Information Privacy Coordinator position. During the 2007 Oregon legislative session, legislation calling for portable, accessible, EHRs was passed. The Healthy Oregon Act, Senate Bill 329, which established the Oregon Health Fund, specifically charges the board “to deliver efficient, safe, and quality health care and a voluntary program to provide every Oregonian with a personal EHR that is within the individual’s control, use, and access and that is portable.” The legislation makes it clear that the Oregon Health Fund Board (OHFB) will need to address patient control issues, including those involving privacy and security. To assist with this endeavor, the governor is transitioning the project steering committee to a Health Information Infrastructure Advisory Committee (HIIAC). The HIIAC will advise the OHFB on health information exchange issues, including privacy and security.

Much of the privacy and security work to date in Oregon has been accomplished by multistakeholder groups primarily organized by hospitals, health systems, and medical associations. Representatives of the state, health plans, and others have been active participants over the past 6 years, since they assembled to solve issues surrounding the implementation of HIPAA. Another significant background issue is the way in which HIPAA was addressed by the 2003 Oregon legislature. Prominent privacy and security attorneys and other experts in the state, drawing mainly from the above-mentioned groups, examined the relevant state laws and then made sure that they conformed to HIPAA.

The Privacy and Security Solutions project has been a catalyst for privacy and security leadership and governance in Oregon. For example, the Metro Portland HIE project predated the Privacy and Security Solutions project, but the work emanating from the project informed the Metro HIE project with respect to privacy and security issues. The transition of the project’s steering committee to an HIIAC was also precipitated by the project findings.

There is now a heightened awareness of patient control issues in terms of privacy and security. However, there is little agreement among individuals about the comprehensibility of HIPAA—some believe HIPAA sufficiently covers the privacy and security issues of health IT and health information exchange, while others do not. The Privacy and Security Solutions project has facilitated an informed discussion on HIPAA among the interested groups and has also provided the impetus for legislative action. The project has aided understanding of the complexity of privacy and security issues and allowed stakeholders to form a more realistic view of issues that need to be discussed before data are exchanged. The project has also encouraged some collaborative efforts across states boundaries with Alaska, California, and Washington. Some of these efforts are addressing similar issues about the interpretation and application of HIPAA.

#### **4.1.27 Puerto Rico**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Puerto Rico initiated an integrated electronic health information system (known in Spanish as SIIS). Puerto Rico has used smart card technology for several purposes including identification and verification of eligibility and a health information storage system for recipients of the Puerto Rico Health Insurance Plan. At the private level, hospitals have been developing their own systems, and some groups of providers are using the electronic interoperable health record of the US Department of Veterans Affairs known as VistA.

The government of Puerto Rico has invested approximately \$52 million in 3 projects: the Smart Card project, the Hospital Information System/Electronic Medical Record (HIS/EMR) project, and the Data Warehouse project, including all necessary infrastructure and support technology. These systems support public operations for people who seek medical assistance in the public medical system.

Meanwhile, the private sector has been developing or implementing its own EHR initiatives. Various hospitals in Puerto Rico have either created their own health information system or purchased one from a vendor. Additionally, *Inmediata* is an automated clearinghouse that follows the Standard Transactional Code Regulation set forth by HIPAA.

##### *Current Health IT/HIE Landscape*

The health IT/health information exchange environment in Puerto Rico continues to have the Puerto Rico Department of Health (PRDH) as the leader in developing the more sophisticated initiatives. A number of private hospitals are working on electronic billing, and some hospitals are focusing on internal hospital exchange. There is limited external electronic health information exchange, with exchange occurring between a few clinics and hospitals (ie, lab and radiology results to their primary care partners).

When the secretary of health took office 3 years ago, a law to foster health information exchange was established, which led to considerable movement in the field. The momentum has slowed since then, and the state project team members see a need to revisit the legislation and the privacy and security policies and technical aspects of health information exchange.

In 2003, the PRDH developed the Integrated Health Information System (IHIS) to ensure that the integration of several health information initiatives was endorsed. IHIS is composed of the following health information initiatives:

- HIS/EMR project for all health care facilities operated by PRDH, integrated with private hospitals via standardized exchanges and an integration engine
- Data Warehouse project to allow effective business transactions with data extracted from all data registries hosted by the PRDH Data Center

- Eligibility project to automate the screening process for the eligibility of Medicaid and the local government-funded insurance
- Telemedicine project linking government-owned primary care centers with Puerto Rico's main Medical Center, operated by PRDH's Telemedicine Center
- Encounter Information project for all primary care physicians offering services to members of the Puerto Rico health insurance plan
- Smart Card pilot project to allow portability of personal health information among all providers (hospitals, labs, pharmacies, clinics, ambulatory centers, physicians, specialists, etc)
- Call Center project to provide continuous support to the entire infrastructure deployed throughout Puerto Rico and to provide direct provider and patient support while using different health IT components
- Computer Center Infrastructure project to improve the center's capacity to provide continuous communication, storage, and support to current technology initiatives throughout Puerto Rico

Also, CMS recently awarded \$4.27 million to Puerto Rico to create and use electronic data exchanges that can validate demographic and socioeconomic data and help reduce fraud and abuse. CMS has awarded a second round of Medicaid Transformation Grants totaling nearly \$52 million to 16 states and Puerto Rico.

### *Current Privacy and Security Landscape*

Most health information exchange initiatives in Puerto Rico are led or guided by PRDH. The territories' laws and regulations are limited on the privacy and security of health information exchange. There is an urgent need to review and update these laws, and the Privacy and Security Solutions project has provided needed momentum in this direction.

The most tangible result of the Privacy and Security Solutions project extension is the development of guidelines for the IHIS initiatives described above. Additionally, the opportunity to collaborate with states in which many Puerto Rico residents reside and move between, such as New York and Massachusetts, has been invaluable, particularly for discussions on issues of information exchange and data-sharing agreements.

Participation in Phase 1 of the Privacy and Security Solutions project enabled the Puerto Rico project team to recognize the need to build consensus about establishing standardized privacy and security policies. The objectives of the implementation project were to:

- Develop of a security and privacy policy model for the Integrated Health Information System.
- Adopt the security and privacy policy for 2 major components of the SIIS: the Hospital Information System/Electronic Medical Record Project and the Data Warehouse Project.
- Develop a health information exchange patient consent clause.

- Formalize the Health Information Exchange Committee.

In November, the project team completed the first draft of the security and privacy policy model for the Integrated Health Information System, and the draft of the health information exchange patient consent clause. The security and privacy policy model for the Integrated Health Information System contains sections on user identification and passwords, patient identification/record matching, patient authorization, access privilege assignment and review, physical safeguards, auditing protocols, and breach notification and sanctions. These models provide SIIS with explicit privacy and security dimensions intended to increase trust and confidence and promote utilization. These models have been adopted as policies by the Hospital Information System/Electronic Medical Record Project and the Data Warehouse Project.

The Privacy and Security Solutions project has increased awareness of the importance and urgency of preparing for health information exchange, and highlighted the many tasks necessary to prepare local health care participants for health information exchange. It has also enabled Puerto Rico to ensure that representatives from all facets of health information exchange participate in essential conversations.

The Privacy and Security Solutions project has influenced health IT initiatives in Puerto Rico in many other ways. For example, stakeholders have a greater awareness of how soon health information exchange is coming and the need for greater involvement. Discussions about changing regulations and laws led organizations to begin thinking about how health information exchange will be accomplished. Puerto Rico is now working to formulate and implement privacy and security solutions and agreements on data sharing with states such as New York and Massachusetts, with an initial focus on sharing public health information. Puerto Rico has proposed the creation of a new entity, a Health Information Exchange Committee, whose mission is to integrate health IT initiatives among the private and public health care providers. This entity will create the necessary guidelines and standards to facilitate health information exchange. It may also endorse the use of standards, ensure stricter security protocols, encourage documentation of patient information electronically, and promote health information exchange.

#### **4.1.28 Rhode Island**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

When the Privacy and Security Solutions project began, the Rhode Island Department of Health (HEALTH) was managing the AHRQ health IT demonstration project on behalf of the community (to build an HIE), and the Rhode Island Quality Institute (RIQI), a public-private collaborative, and HEALTH were in an advanced stage of collaboration. In addition, the governance structure for Rhode Island's HIE (RI HIE) was in place: policy and legal,

consumer engagement, and technical work groups were all associated with the AHRQ health IT project and leveraged to the Privacy and Security Solutions project work. Integrated delivery networks (IDN) and some private provider groups had EHRs, including 1 IDN with longitudinal records, and most were involved in the Rhode Island HIE initiative. Surescripts was piloting medication history exchange in national projects, and EHR RI, a for-profit organization, had begun offering subsidized health information exchange and EHR for providers with e-Clinical Works as a vendor partner. These initiatives, and others, are described in greater detail in the following paragraphs.

In 2004, AHRQ awarded HEALTH a 5-year contract to conduct a state and regional health IT demonstration project to develop and implement a statewide interoperable HIE system. HEALTH also received a 1-year InformationLinks grant to identify and implement laboratory and immunization data standards for use in the RI HIE and to migrate public health data from HEALTH to the HIE. HEALTH has worked closely with local health organizations, private physicians, public health agencies, policy and legal experts, consumers, and a technical vendor to design and develop the RI HIE. RIQI, a not-for-profit corporation that serves as a collaborative of high-ranking leaders from both the private and public sectors, has provided the governance structure for the RI HIE. RIQI has supervised a number of committees that guide statewide health IT initiatives, such as the steering committee for the HIE, the RIQI Policy and Legal Committee, and the RIQI Consumer Advisory Committee. In the public sector, Rhode Island Governor Donald L. Carcieri has set “Anytime, Anywhere Health Information” as one of his health care policy priorities. The state plan for achieving this goal has been monitored by the cabinet-level Directors Healthcare Group, chaired by Rhode Island’s Health Insurance Commissioner. A health IT subgroup was created and staffed by HEALTH. The governor’s support of health IT has brought visibility and political will to accelerate ongoing public-private efforts in the state.

Following are other significant health IT efforts in the state that have been concurrent with the Privacy and Security Solutions project:

- HEALTH operated KIDSNET, an integrated child health information system, and Millennium, a statewide clinical laboratory information system.
- Lifespan, a large IDN, operated a lifetime electronic clinical record system and e-prescribing (eRX) solution for ambulatory and inpatient care providers across the state.
- Care New England, a large IDN, has integrated disparate systems into an EHR.
- Surescripts, an eRX network operator, has piloted a medication history exchange in Rhode Island (and other states).
- East Side Clinical Laboratory provided a web-based electronic interface for lab reporting.

- Quality Partners of Rhode Island, the state's Quality Improvement Organization, administers the DOQ-IT project, provided technical assistance to providers interested in purchasing an EHR.
- EHR of Rhode Island offered group purchase agreements to subsidize EHR pricing for providers.
- Rhode Island Primary Care Physician Corporation developed and operates an EHR for its network of Rhode Island providers.
- Blue Cross Blue Shield of Rhode Island has offered a pay-for-performance program as an incentive for EHR adoption.

### *Current Health IT/HIE Landscape*

In Rhode Island, there is significant energy and focus to promote the authorized exchange of health information among health care providers. Much of the work to advance electronic health information exchange is taking place among existing medical trading partners. At the same time, major collaborative initiatives are being jointly coordinated by HEALTH and RIQI, a public-private collaborative. Through these collaborative health IT initiatives, Rhode Island seeks to achieve the vision of a statewide health information exchange system that can improve the quality, safety, and value of health care provided in Rhode Island.

In 2006, the governor and legislature authorized the state to fund a proportionate share of the total capital and operating costs through a revenue bond to the RHIO. The percentage of funding would be based on the percentage of covered lives for which the state provides health insurance. The funding is contingent upon the other insurers in the state contributing their fair share and the state designation of a RHIO through an open bid process.

The RI HIE is under active development amid a variety of continuing market-driven initiatives. The state is in the final stages of designating a RHIO to serve as the operating and shared governance entity for the RI HIE, once implemented. The state issued an RFP for Rhode Island RHIO designation and, as of November 2007, is reviewing proposals with the goal of designating an HIE as the state RHIO. For the final 6 months of 2007, the team has focused on safeguards development for health information exchange that would support the newly designated RHIO. Specifically, the team is reviewing policies that would be initiated within the next 6 months.

Because of the interactions among these prior and ongoing initiatives, it is sometimes difficult to attribute outcomes specifically to any one initiative. However, within this context, Privacy and Security Solutions project work has offered important contributions to planning and development by supporting a level of detailed analysis and insight that would not otherwise have been readily attainable.

The project has led to enhanced awareness and relationships by exposure to many current collaborative efforts in other states. During the assessment of variation, Rhode Island was able to start a dialogue with groups that were not currently involved in the statewide health

information exchange initiative, including mental health/substance abuse providers, nursing homes, emergency rooms, and radiology facilities. Many one-on-one meetings with stakeholder groups were valuable in establishing communication and support.

The extension in 2007 allowed Rhode Island to delve deeper into privacy and confidentiality policy issues in the state and has significantly advanced privacy and security issues related to health information exchange development, including the development of draft legislation. Rhode Island has realized broad stakeholder and consumer endorsement through additional protections for data.

### *Current Privacy and Security Landscape*

State and federal laws and a wide range of related organizational policies define privacy, confidentiality, and security protections for the exchange of health information in Rhode Island. Relative to the emerging Rhode Island Health Information Exchange (RI HIE), the Privacy and Security Solutions project was well-timed to help address stakeholder needs to: (1) understand how the current legal framework applied to this mechanism; and (2) assure that consumers had an active role in determining how and to whom their protected health information would be disclosed through the RI HIE. Because activities preceding the Privacy and Security Solutions project work were in full alignment with the project's goals, the added structure, process, timeline and resources provided by the Privacy and Security Solutions project accelerated the state's ability to make significant gains.

Following the examination of the privacy and security landscape in Rhode Island through the analysis of laws and policies and the variations in current health information exchange practices, leadership for the Privacy and Security initiative made a decision to set the privacy and security agenda for solution development in the context of the emerging RI HIE system. This approach was believed to be the best vehicle for broad collaboration (including active engagement of consumers) and statewide implementation of strong privacy and security policies and practices for the electronic exchange of health information. Thus, the Privacy and Security Solutions project has been fully integrated into the state's health information exchange activities.

During the project, the team has built and sustained momentum toward state-level health information exchange. The team is focusing its efforts on 4 privacy and security domains: (1) data protections, (2) patient record matching and merging, (3) authentication, and (4) auditing.

Rhode Island's implementation project has produced 3 deliverables and 2 works in progress. The 3 deliverables from the 6-month implementation phase include draft guidance for implementation of privacy and confidentiality safeguards in the RI HIE; the master RI HIE policy, technical, and operations development workplan; and consensus patient authorization principles and policy for the RI HIE environment. The works in progress

include an operational approach for the RI HIE authorization (consent) model and the final draft of proposed RI HIE legislation.

The major point of evolution in Rhode Island's privacy and security landscape centers around community demand for more stringent protections for health information exchange through the RI HIE than are currently required for routine organization-level exchanges. In support of this demand, the Rhode Island Privacy and Security implementation project proposal targeted the development of privacy safeguards in coordination with technical implementation of the RI HIE system. A broad perspective was needed to catalog all privacy safeguards and understand their impact on the work plan for the technical development of the RI HIE while the in-depth focus was on the most critical near-term privacy protections to be implemented: (1) the RI HIE patient authorization policy; and (2) the development of new legislation for the RI HIE. Overall, tremendous progress occurred in 6 months, a testament to the groundwork that was laid and the intense efforts of many stakeholders.

The Privacy and Security Solutions project has had a significant impact on the team's choice of methods to document patient permission to access records. After a close analysis of state and federal law, enabled by the Privacy and Security Solutions project, a model was adapted to include an affirmative consent requirement before transferring protected health information to the RI HIE from its originating source. This additional consent created a 2-part process for gaining patient permission for the transfer and release of health information. The team found that stakeholders wanted this feature to be more stringent to account for differences in legal interpretation of state laws and to build consumer confidence in the health information exchange disclosure policies.

Although legislation was an early consideration in the RI HIE development because of the need for a broad set of health information safeguards, the details provided by the Privacy and Security Solutions project team for the authorization policy accelerated Rhode Island's legislative initiative (draft legislation to protect information in the HIE). Understanding the stakeholder requirements relative to what is provided by law helped the team assess various aspects of legislation.

Rhode Island is still in the preliminary stages of working toward interstate exchange of health information. The state has been engaged in a dialogue with Connecticut and is in regular communication through quarterly face-to-face meetings with other New England states, but the focus of most activities has been within the state.

Rhode Island has a governance structure for the current AHRQ health IT/health information exchange project (and the Privacy and Security Solutions project), which includes the board and management of RIQI. The state is actively pursuing formal designation of a RHIO for long-term governance and operation of the RI HIE. The proposed legislation would identify a regulatory agency for the HIE and create a Policy Advisory Commission to serve as an independent advisory commission. The advisory commission would advise the named

regulatory agency and the RHIO about data exchange and use issues. The governance structure addresses overarching issues that include privacy, confidentiality, and security.

#### **4.1.29 Utah**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Utah has a long history of health care stakeholder involvement in health IT/health information exchange activities. Before the nationwide adoption of the HIPAA electronic data interchange standards, insurers, hospitals, physicians, state government, and other stakeholders in Utah over several years developed a consensus on standards for the exchange of administrative data necessary to process electronic claims. The trading partners in this project eventually became the nonprofit Utah Health Information Network (UHIN) Board of Directors, which now comprises representatives from 17 insurers, provider organizations, and other interested parties, including state government.

In 2004, AHRQ awarded UHIN a multiyear contract to function as a RHIO. Specific planned clinical data sharing projects include laboratory results, chief complaint, chart notes, hospital discharge notes, continuity of care records, and e-prescribing. In addition, UHIN is in the process of evaluating proposals for a master patient index to assist in the accurate identification of patient information in these exchanges. Work groups of volunteers from the community of stakeholders interested in these exchanges are actively working to develop the standards that will serve as the basis for these exchanges.

In December 2005, the Utah Department of Health obtained funding from the Robert Wood Johnson Foundation InformationLinks project for the Utah Network for Electronic Public Health Information (UNIFY) initiative. UNIFY has begun a yearlong planning effort to develop a business plan for public health participation in clinical exchanges. UNIFY has the goal of evaluating business practices for all of the potentially valuable exchanges between the clinical care sector and public health, but is especially focused on surveillance of reportable diseases, vital records, immunizations, and newborn screening. Other active health IT efforts of the Utah Department of Health include the Utah Patient Safety Program, reengineering of the MMIS, immunization registration, and the CHARM child health integration program. Additionally, the Utah Bureau of Epidemiology is collaborating with UHIN to expand the Remote Outbreak Disease System, which was implemented during the 2002 Salt Lake City Winter Olympics to conduct syndromic surveillance in Utah emergency rooms and pharmacies.

HealthInsight, the primary partner of the Utah Department of Health on the Privacy and Security Solutions project, entered into a 3-year contract with CMS in mid-2005 to help physicians assess the benefits and overcome barriers to adopting and using EHRs and other health IT. As part of the DOQ-IT project, HealthInsight is working with physicians to

understand the potential of health IT, such as e-prescribing, electronic management of lab results, electronic medical image storage and transmission, and deployment of full EHRs for improving care in ambulatory settings, where most patient care is provided. HealthInsight will encourage adoption of health IT by helping physicians in Utah and Nevada learn about the clinical advantages of using EHRs for managing and improving care.

### *Current Health IT/HIE Landscape*

The majority of the health IT/health information exchange initiatives in the state are being conducted by the Utah Department of Health, which oversees the UHIN. Several new state initiatives have been launched concurrently with the Privacy and Security Solutions project. The Utah Department of Health has recently created the Public Health Information database, which contains all hospital discharge information now available to the Department of Public Health.

Tangible successes so far include reviewing a state-sanctioned common language form to be made available to all physicians and a request to put together the draft requirements for UHIN's governance. Utah is also seeking consensus for the RHIO exchange with regard to designing standards, both policy and technical. The state is also working on establishing a standard of practice for health information exchange.

The project also encouraged the state project team to work across states in formulating and implementing electronic health information exchange policies and practices. The biggest reason for this outreach is that Utah is a regional treatment trading area, with many patients at 1 facility (often up to 40%) coming in from out of state. Consequently, the transfer of information across state lines can potentially be a major issue, especially if the receiving hospital requires information from other state public health department.

The Privacy and Security Solutions project has also influenced other health IT initiatives in Utah by increasing the recognition for the need to develop standards. Also, it has moved the issues of privacy and security to the foreground. Previously, privacy had been a taboo. Indeed, consumers were able to stop some health IT efforts because of fear of privacy issues; before the project was initiated, industry representatives wanted to deal with the issue behind closed doors. The project has elevated privacy and security and made it an issue. The project's steering committee continues to make recommendations to state government, and it now makes recommendations on privacy and security policy issues. The steering committee has agreed it is important to carry that voice forward.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project has provided Utah an opportunity to begin to standardize privacy and security policies and practices critical to widespread electronic clinical data exchange. The systematic review of the practice and policy landscape conducted in the first phase of the project led to the identification of both real and perceived

privacy and security policy variation and laws that serve to inhibit appropriate interoperable health information exchange. Utah proposed a work plan geared to dispel myths about perceived constraints, and prepare community stakeholders to make business decisions that support progress toward appropriate interoperable healthcare information exchange.

Implementation activities were a targeted and coordinated effort to begin the process to establish Utah's *standard of practice* for the secure and private exchange of safeguarded health information. The Utah project team deployed a 3-tiered approach that included assessing the need for a common/model Notice of Privacy Practice (NPP) policy, educating physicians and their office staff about allowable disclosures under Utah law, and decision tools for policy-recommending bodies.

The Utah project team conducted an analysis of NPP policies to identify similarities and / or differences in existing policies that may suggest any reasoning for this misunderstanding. Targeting existing policy allowed stakeholders to focus on the source of variation and work toward a common understanding and uniform interpretation. The analysis examined 21 unique policies collected during the first phase of the project and compared them to the HIPAA required elements [45 C.F.R. §164.520 (b)(1)] and to *Model Privacy Policies and Procedures for Health Information Exchange* (Connecting for Health, 2006). Each policy was reviewed for consistency in language, organization, and length with a focus on noted uses and disclosures. Results indicated that physicians/clinics policies were less likely to include all the HIPAA required elements in the patient notice. The inconsistency of the group, especially the handful of unusually low scores, suggested that some of the submitted policies may not be recently updated or composed by professionals. Results did not implicate the policies as the source for the misinterpretation between "consent to treat" and "authorization to disclose." Plans are under way to make available to the provider community the matrix created to assess the policies. This tool may be made available to physicians/clinics to conduct a self-assessment of their own policy.

The project team also identified the goal of dispelling myths and misunderstanding by educating the provider community about patient consent to treat. Additionally, the team established a principle that acceptable sharing of health information for treatment purposes must include both the clinician and their office staff. The education tool kit created for the health care provider community targets allowable disclosures according to HIPAA's General Provisions for treatment, payment and health care operations with an emphasis on treatment purposes. The education tool kit has been approved by Utah's HIPAA Taskforce and will be disseminated by counsels for the respective entities. An electronic version of the toolkit will be available to the general public via the Unify-PS site.

Facilitating the secure exchange of safeguarded health information for treatment required clarifying the legal requirements under Utah and federal law with policy and practice. The impact assessment tool was developed for use by standing policy committees to review a

recommended statutory and regulatory change under consideration to create safe harbors for health information exchange. Providing such committees with a practical tool for assessing policy change may prevent or minimize further variation in privacy and security requirements by allowing standing policy bodies to consider the impact of their recommendation prior to finalizing a decision.

The Privacy and Security Solutions project has led the team to identify or interact with stakeholders that might not otherwise have been involved, such as the Utah Trial Lawyers Association and the American Civil Liberties Union, and with numerous consumer support organizations. These interactions have been extremely beneficial. Finally, this project has also stimulated the creation, advancement, or endorsement of health information exchange in Utah.

#### **4.1.30 Vermont**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

Vermont has been working toward a vision consistent with a nationwide health information network since 2004. Vermont Information Technology Leaders (VITL), a nonprofit public-private RHIO incorporated in 2005, was charged by the legislature with convening stakeholders interested in health IT to assist in developing a statewide health IT plan by 2007. At the start of the Privacy and Security Solutions project, VITL expected to have the infrastructure and agreements in place to implement an EHR network across the state within 5 years. These plans have since been revised, as described later in this section. Health concerns in the state have helped to drive these initiatives. Of particular concern is the increasing number of individuals with chronic conditions in Vermont. According to *Vermont Blueprint for Health*, Vermont's chronic care initiative, 51% of all Vermont adults have 1 or more lifelong health conditions that require ongoing medical care (Vermont Department of Health, 2007). That number jumps to 88% when only adults aged 65 or older were considered.

A key to VITL's success has been the representation on the Board of Directors or advisory committees of each of the stakeholders engaged in information sharing and health IT activities in Vermont. The following list summarizes the current information sharing and health IT activities across stakeholder groups in the state:

- The NorthEast Community Laboratory Alliance is a regional network of community-based clinical laboratories. The network currently serves 13 of the 14 acute care hospitals in Vermont. So far, the network has coordinated reference testing, developed an active test exchange program, implemented a common system for test ordering and reporting, created a business plan, and developed disease management testing strategies.
- The Vermont Diabetes Information System is a registry-based decision support and reminder system for primary care physicians and their patients with diabetes.

- Vermont Chronic Care Collaboration (V3C) Disease Registries is a Breakthrough Learning Series Collaborative sponsored by the Vermont Program for Quality in Health Care.
- Fletcher Allen Outreach Clinical Messaging System is a multiyear project that will build the necessary infrastructure and applications to connect hospitals and their local physicians. The system will allow orders, results, clinical data, and patient information to flow between each site using intelligent interfaces, document image exchange, and a web application.
- OBNet is a web-based obstetric delivery registry application developed in 2003 through a joint effort between Fletcher Allen Health Care and Dartmouth Hitchcock. The primary objective of OBNet is to improve obstetric and early infant care in Northern New England.

In addition to these health IT activities, the Vermont Agency of Human Services uses Health Information Systems through its National Electronic Disease Surveillance System, Vital Records, Immunization Registry, and Laboratory Information Management System.

### *Current Health IT/HIE Landscape*

The health IT/health information exchange environment continues to be innovative and aggressive in Vermont.

Following are some activities that have recently taken place in Vermont:

- ***Vermont Health Information Technology Plan.***<sup>9</sup> In July 2007, VITL published a comprehensive statewide health IT plan, with input from a work group of more than 30 stakeholders. The Vermont Health Information Technology Plan identifies a set of 4 core objectives for a 5-year planning cycle:
  - Encourage and enable the deployment and use of EHR systems within the state to increase the amount of health information that exists in electronic form.
  - Establish and operate the infrastructure necessary to promote a secure electronic health information exchange to achieve the plan's vision.
  - Empower consumers to take an active role in electronic health information initiatives in Vermont.
  - Enable public health agencies to leverage health IT/health information exchange investments to monitor and ensure the public's health more transparently and quickly.
- ***EHR Pilot.*** Building on what it learns through the pilot project, VITL plans to help the state's 318 primary care physicians who work in practices not owned by hospitals to acquire EHRs. The 3-year cost of that project is projected at \$25 million. A source for the funding has not been identified, but VITL officials said they expect the legislature to take up the issue in the coming session. Although a long-term funding source has not yet been identified, an interim fund was created by the legislature for the EHR pilot. VITL has also issued a request for information and a request for applications as part of the pilot.

---

<sup>9</sup> Additional information on VITL can be found at the website (VITL, 2007).

- ***Pilot Program on Medication Histories in Emergency Departments.*** VITL's first pilot project is already running in the emergency departments of 2 local hospitals. It delivers patient medication lists within seconds of the patient's arrival—even if the patient has never visited that hospital before. VITL and GE Healthcare will be working together to develop and implement other standards-based health IT projects.
- ***Chronic Care Information System (CCIS).*** As part of the state's Blueprint for Health program, VITL and the Vermont Department of Health are developing a web-based disease management system designed to help physicians meet the challenges of providing chronic disease care. Together, the CCIS and the Medication History pilot are part of a long-term strategy to incrementally build health information exchange infrastructure in the state.

A report by the US Department of Health and Human Services' Office of Inspector General found that Vermont is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Iowa, Kansas, Louisiana, Mississippi, Wisconsin, and Wyoming.)

The most tangible outcomes of the Privacy and Security Solutions project for Vermont include the progress made by a focus group on other consumer outreach activities and the significant contributions made to the privacy and security chapter for the statewide health IT plan. The team has also realized that enhanced consumer engagement and a consumer focus group within the Privacy and Security Solutions project provided the foundation for a subsequent telephone study to elicit consumer opinions.

The Privacy and Security Solutions project work has always been a part of the ongoing, larger body of work within Vermont. The Privacy and Security Solutions project is the privacy and security part of the VITL work. Also, the Privacy and Security Solutions project influenced the governance section of the health IT plan published in 2007 (Vermont Information Technology Leaders, 2007). The report was written between October 2006 and June 2007, and the Privacy and Security Solutions project participants played a major role. The privacy and security chapter of the plan was highly influenced by the project work.

This project also led the team to identify or interact with stakeholders that might not otherwise have become involved, including the Vermont chapters of the ACLU and AARP, as well as other consumer-oriented groups. The Privacy and Security Solutions project has helped solidify relationships with stakeholders.

The governance structure for VITL is in place (board of directors, subcommittee on privacy and security). Team members have observed that some states have an independent, free-standing privacy and security governance body and are examining the possibility of having

such a body in Vermont, along with other alternatives. They have recognized a healthy tension between the board of directors and some Privacy and Security Solutions project proposals.

### *Current Privacy and Security Landscape*

As a result of the assessment of variation, analysis of solutions, and implementation planning, education and consumer outreach were identified as critical components of building successful health information exchange. To work toward this goal, the Vermont team developed content for VITL's website and engaged with VITL's Consumer Group. Throughout the 6-month implementation period, VITL maintained, promoted, and developed new content for its website.

Vermont's implementation project has contributed to security and privacy related efforts in 4 broad areas—consumer engagement and education, infrastructure, technology solutions, and policy and legislative development—as well as a national collaborative effort related to patient consent. These priority areas were selected from a broader range of options outlined in Vermont's Final Implementation Plan Report as projects that could be completed within the 6-month timeframe and would advance health information exchange in the state. The tasks are closely related to current health information exchange activities in Vermont, especially these initiatives led by VITL. VITL is the exclusive operator of the state's health information exchange network, as designated by the Vermont General Assembly. Thus, the Privacy and Security Solutions project team works closely with VITL to ensure projects are complementary and to advance private and secure health information exchange. The project team has identified the following 5 key outcomes emerging from the implementation phase projects:

- documented feedback from the VITL Consumer Group on consumer engagement and policy;
- a statewide potential project and data source list, identifying priority areas consistent with Vermont's Health Information Technology Plan (VHITP) project selection strategy and including privacy and security-related infrastructure needs;
- a multistate analysis of biosurveillance data sets to help understand the privacy implications for cross-state exchange;
- draft implementation documents on Integrating the Healthcare Enterprise (IHE) Basic Patient Privacy Consents (BPPC) for the Medication History Project and the Chronic Care Information System (CCIS); and
- a legislative priorities white paper.

These efforts are discussed in greater detail in the following paragraphs.

Discussions with consumers and consumer advocates led the Vermont team to note that if patients do not feel their information is private and secure, they may opt out of health information exchange, ask a physician not to take notes, withhold important information, or

choose not to seek health care at all. To address this issue, the VHITP proposed a framework in which (1) the health information exchange network will adopt policies and procedures consistent with the requirements of the HIPAA Privacy and Security Rules; (2) the health information exchange network will actively seek to be a leader in the state and amongst its various member organizations in tackling the large, inter-organizational and cross-state privacy and security challenges that are constantly evolving both at the national and local level; (3) the health information exchange network will create a strategy to help providers meet their legal obligations, especially in those cases where the obligations are complicated by cross-provider, cross-state, or health information exchange boundaries; and (4) the health information exchange network will implement consumer education initiatives on privacy and security issues.

VITL organized a consumer group conference call, a continuation of a series of 3 calls conducted during the spring. Feedback from the spring calls was used in developing the VHITP. The team documented possible strategies for formalizing a consumer advisory structure and prepared to ask the consumers for their input.

Overall, the strongest sentiment that emerged from the discussion was that a VITL ombudsman could significantly help in meeting the challenge of consumer representation and protection in health information exchange. The consumer representatives discussed 3 challenges that hinder these efforts:

1. Many of the security and privacy issues in health information exchange are abstract.
2. It takes a great deal of effort to be current on all of the activities, acronyms, people, laws, and data in this area. Many of those who have the time to stay closely involved are already part of the VITL organization or one of its nonconsumer stakeholders.
3. Initiatives designed to collect comments, observations, and advice from consumers can lose influence and can lose participation over time if it is not clear that the feedback is having an impact.

Though the ombudsman was the dominant recommendation discussed during the call, advice was solicited from the callers on other strategies as well. The representatives saw value in other consumer involvement strategies, as long as their limitations are recognized. A way of formalizing the groups' feedback and putting it into the official record is important. It is important for the group to be able to present this to the appropriate governing bodies, such as the VITL executive board or VITL committees. As a result of these conversations, recommendations regarding the funding of an ombudsman's position were included in the team's legislative agenda for the upcoming year.

In addition to their work with consumers, the team also observed that, historically, stakeholders have had difficulty in linking potential health information exchange projects with potential data sources. To address this, the team created a matrix of possible

opportunities by cross-listing data sources (such as payors, hospitals, laboratories, pharmacy benefits managers, etc.) with existing infrastructure. A website was created to host the matrix and allow for members of the newly formed VITL Project Review Committee to collaborate on it.

Vermont has also completed a multistate analysis of biosurveillance data sets to help understand the privacy implications for cross-state exchange. Having recently contributed to a proposal for CDC's Biosurveillance Situational Awareness request for proposals, as part of the North East Biosurveillance Collaborative (NEBC), VITL felt that there was an opportunity to study some of the security and privacy issues related to biosurveillance and health information exchange as a part of the Privacy and Security Solutions project work. Therefore, one of the Privacy and Security subprojects that VITL proposed was related to biosurveillance, to pursue the following biosurveillance goals:

- Analyze and understand the privacy implications in the minimum data set and in optimal data sets being developed to support biosurveillance situational awareness.
- Work with neighboring states to harmonize these data sets and understand interstate privacy implications.
- Examine the privacy implications of sharing public health information with other states in New England.

The first step towards achieving the goals was to examine the data elements that make up the Biosurveillance Minimum Data Set (MDS) and how they compare to the data elements currently being submitted to the Vermont Department of Health (VDH) by the 6 Vermont hospitals participating in the biosurveillance program. The overall purpose of this document is to lay the groundwork for future efforts in Vermont to implement a use case for biosurveillance, both within Vermont and for sharing biosurveillance data with neighboring New England states, by documenting the data elements and data formats currently supplied to VDH for biosurveillance and the extent to which this supplied data conforms to the Biosurveillance MDS.

As part of their Privacy and Security Solutions project work, Maine and New Hampshire are pursuing similar goals. While the Vermont analysis goes into more depth on the biosurveillance data elements, the Maine/New Hampshire analysis is broader, focusing on reportable diseases and corresponding case reporting data elements in addition to the biosurveillance data elements. The 3 states plan to work together in 2008 to continue to explore the possibility of cross-border exchange of public health data.

The Vermont team also sought to address a central barrier to intra- and interstate health information exchange: collecting, communicating, and applying electronic consent information in a standardized way. The standard selected for this work was the Integrating the Healthcare Enterprise (IHE) Basic Patient Privacy Consents (BPPC). IHE Profiles are essentially recommendations for how to use existing standards, many of which have been

recommended by the Health Information Technology Standards Panel (HITSP). In the case of patient privacy consents, these requirements must reflect the needs of state stakeholders and must also be sensitive to cross-state exchange challenges.

The BPPC process forced the team to clarify and formalize their consent policies because it required them to define and number policies. In addition, the process provided the team with a new way of expressing consent policy to stakeholders and encouraged them to think about consent as a document in the health information exchange.

The end result of the team's analysis were 2 draft documents that present the consent policies for the Medication History Project and the CCIS using the IHE BPPC methodology, and show how BPPC documents could be created and stored in the exchange for these projects. They illustrate ways in which the 2 projects could expand or modify their consent policies to take advantage of BPPC to provide more flexibility and control for the patient and more efficiency and more complete information for the physician. In December, the team plans to finalize the drafts and utilize the CCIS document to assist with efforts in developing business associate agreements.

Clarifying the privacy and security issues related to electronic health information and health information exchange for patients and providers has the potential to accelerate the providers' full participation in the health information exchange, by increasing the percentage of patients who opt in to the exchange and by streamlining the processes to do so. It is generally recognized that health information exchange educational and policy initiatives alone may not be sufficient to fully address privacy and security barriers for the long term, and that legislation may play a vital role in the coming years. The Vermont team has drafted a white paper on legislative priorities that will serve as a road map during the next legislative session. The topics include:

- funding and role of the ombudsman;
- strengthening enforcement; and
- clarifying consent law and emergency access rules.

The proposal related to an ombudsman came directly from the consumer groups' recommendations, while the other 2 emerged from the legal analysis completed by the team in the initial phase of the Privacy and Security Solutions project. With respect to enforcement, the team noted that a functional enforcement mechanism may help consumers feel more secure in allowing the electronic transfer of their health information. State law may also need to be modified to clarify the legal situations of consent and emergency access within an electronic environment.

The tasks conducted during this project are closely related to current health information exchange activities in Vermont, and part of a larger strategy to achieve the vision of secure and private health information exchange in the state. The Vermont team plans to participate

in a collaborative working to address consent in cross-state exchange in 2008. In addition, they will continue to work with VITL to ensure the development of private and secure health information exchange in Vermont.

#### **4.1.31 Washington**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In 2005, the Washington State legislature passed a bill (Substitute Senate Bill 5064) requiring the development of a state strategy for the adoption and use of EMRs and health IT to be consistent with emerging national standards and promote interoperability of health information systems. The Washington State Health Care Authority (HCA) convened a Health Information Infrastructure Advisory Board (HIIAB) to develop this strategy. The HIIAB was charged with making specific recommendations to the legislature for a strategy and plan designed to (a) encourage greater adoption and use of EMRs and health IT among the state's health care providers and (b) reduce medical errors and enable patients to make better decisions about their own health care by promoting access to medical records. The legislature called for the identification of obstacles to an effective health information infrastructure in the state, provision of policy recommendations to remove or minimize these obstacles, and development of health care purchasing strategies that would provide incentives to providers and organizations to adopt effective health IT. The legislature noted specifically that the strategy and plan must preserve the privacy and security of health information, as required by state and federal law.

Governor Gregoire developed a 5-point strategy for increasing quality and reducing the cost of health care purchased by state programs in Washington. One of the points in the strategy focuses on making better use of health IT. Specifically, the governor has set a goal for implementation of EMR systems in all of the state's hospitals by 2012, has directed the HCA to implement pilot projects for reimbursement incentives to providers and organizations that adopt health IT, and is planning the launch of a public employee health plan that will serve as a model for the state on electronic data interchange.

A number of organizations and initiatives were established to address various aspects of electronic health information exchange, including the following:

- The Puget Sound Health Alliance was formed in December 2004 as a public-private partnership of more than 160 organizations and has created a sustainable leadership coalition among patients, providers, purchasers, and health plans to improve quality and reduce the cost of health care across King, Kitsap, Pierce, Snohomish, and Thurston counties. A key goal for the alliance is to facilitate the development of interoperable health IT in the most populous region of the state.
- In 1996, the Community Health Information Technology Alliance (CHITA) was formed to help facilitate collaborative health IT planning initiatives in the region. CHITA

members include providers, health IT vendors, health plans, and government agencies. CHITA is a program of the Foundation for Health Care Quality. CHITA has engaged in a number of projects relevant to health IT privacy and security.

- The Washington Healthcare Forum is a coalition of health plans, physicians, hospitals, and purchasers that has joined together to improve the health care system. The forum's contributions to health system improvements include development of guidelines for administrative simplification, creation of local implementation guides for national standards, development of quality measures, and creation of OneHealthPort. OneHealthPort provides health care professionals a single and secure way to sign on to local health care sites and online services.
- As part of its Medicare Quality Improvement Organization contract, Qualis Health is assisting nearly 100 physicians in Washington in selecting and implementing EMRs. One goal of this project is to contribute to an infrastructure that will support interoperable health information exchange by assisting practices with capturing and sending patient information through EMRs to a centralized data repository on a set number of quality measures.
- The South Sound Health Communication Network is a RHIO being formed in Tacoma, Washington, that is sponsored by Northwest Physician Network and the Pierce County Medical Society. The South Sound Health Communication Network is a secure, web-enabled communications platform that provides electronic access to medical record information for all providers and their patients, regardless of the medical information's origin in the community.
- PeaceHealth, a 6-hospital network based in Bellevue, Washington, has developed a community health record over the past 10 years that enables independent medical groups in Alaska, Oregon, and Washington to access patient data. This network also links laboratory services and competing hospitals in Eugene, Oregon, and Longview, Washington.

### *Current Health IT/HIE Landscape*

As the proposal to join the Privacy and Security Solutions project was developed, the state project team joined with the Washington State Health Care Authority, which was tasked by the governor's office to create the HIIAB to oversee the progress of health information exchange for the state. The Washington state legislature has since convened and approved more than \$4 million for the HIAAB to develop a consumer-centric health record banking model. The Washington project team is integrated with the HIIAB and is consulting on privacy and security issues. Team members have been attending the HIIAB meetings, which take place once a month. Members of the HIIAB and stakeholder panel represent a variety of other health information exchange initiatives, such as the Whatcom county project on personal health records in hospital emergency departments. The HIIAB meets to discuss these multiple initiatives once a month, which provides a forum for bringing together these separate initiatives. The project has a formal designation from the HIIAB to be the group that reports and focuses on privacy and security. The Privacy and Security Solutions project team is the official Privacy and Security Work Group of the HIIAB.

The Privacy and Security Solutions project stimulated the creation, advancement, or endorsement of HIEs in Washington in the following ways:

- The government has been offering grants as part of the governor's 5-point strategy to encourage EHR adoption.
- Qualis Health has a contract with CMS to help smaller physician offices adopt and implement EHRs in Washington.
- By working within the Authentication and Consumer Engagement Collaborative work groups, the project team members can offer some information and knowledge that might be helpful to health information exchange projects across states.
- At the last HIIAB meeting, members discussed the point that all of the technical issues require consumer/stakeholder buy-in. This project is the best tool for ensuring that the configuration, policies, and procedures of health information exchange in Washington are in line with consumers' needs.

In October 2007, another \$1 million in grants was awarded by the Washington Health Information Collaborative, a public-private partnership promoting greater use of health IT, to small physician practices and critical access and rural hospitals. Since 2005, the collaborative's awards to health care providers total \$2.2 million for acquiring, implementing, and expanding health IT to improve health care efficiency and effectiveness. In 2007, funding for the awards was provided by two \$500,000 contributions from First Choice Health and the Washington State Health Care Authority. Also participating in the collaborative are Qualis Health and the Puget Sound Health Alliance.

### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project has heightened awareness of the degree of variability in privacy and security practices across the state. There is little consensus on interpretation and application of HIPAA privacy and security rules and other state and federal laws, leading to a wide range of business practices in both paper-based and automated systems. This has increased interest in establishing uniform standards that will reduce the degree of variation while continuing to provide flexibility in how users/entities implement the standards.

Stakeholders in Washington share a substantial amount of knowledge and understanding of privacy and security issues related to health information exchange, as witnessed by the many health IT and health information exchange initiatives ongoing across the state. The longstanding frustration among stakeholders has been the inability to promote adoption of uniform standards among those involved in health information exchange projects. Refusal to adopt standards stems from a genuine fear that the rules will change once investments have been made and resources have been expended. Stakeholders are demanding a clear and legal definition of the health information exchange standards and assurance that all participants will play by the same rules.

Since completion of the first phase of the project, the Washington project team has achieved the following results:

1. A governance structure has been established to oversee implementation of project recommendations through the HIIAB.
2. HIIAB has been funded by the state legislature through June 2009 to build a consumer-centric health record banking model. To take steps toward building the health record bank, HIIAB created 3 committees and 3 subcommittees. One subcommittee is charged with developing privacy and security recommendations for the health record bank during the next 18 months, continuing the work initiated in Phases I and II of the Privacy and Security Solutions project.
3. Minimum technical data standards for user/entity authentication have been developed. Additionally, a framework has been established to continue development of privacy and security standards for authorization, access, and transmission security and exchange protocols. The user/entity authentication minimum data standards address exchange agreements, exchanging authentication data, and audit trails. Use of second-factor authentication was deemed a preferred practice, but not recommended as part of the minimum authentication standards. The minimum standards are voluntary.
4. Incentives to promote early and continuous adoption of the privacy and security technical standards through safe harbor-style protections were recommended as a mechanism to relieve perceived barriers to health information exchange deployment while at the same time increase patient safety, and expand consumer protections through broad voluntary application of the minimum standards.
5. A framework to encourage consumer participation in Personal Health Records (PHR) and Health Record Banking (HRB) has been developed that address the following needs:
  - a. Education to assist with consumer decisions to opt-in to create and use PHR and HRB.
  - b. Consent forms to control use and disclosure of personal health information and authorization to add data to one's PHR and HRB.
  - c. Parameters for consumer controlled security levels for PHR and HRB.
  - d. Standard data set for health record banking.
  - e. Incentives to encourage individual and organizational participation in PHR and HRBs through financial rewards, improved safety, and efficiencies/reduced costs, each with targeted messages to address the specific needs of various demographic segments.
6. Washington State stakeholder involvement with the Privacy and Security Solutions project activities has been evident, with stakeholder participation on technical advisory panels, independent collaborations with other states in the project, and participation in 2 multistate collaborative efforts on privacy and security for health information exchange that focus on consumer engagement and standards adoption. The coordination of efforts with various states that face similar health information

exchange issues as Washington State are valuable for gaining knowledge and increasing efficiencies.

The Privacy and Security Solutions project has encouraged Washington to work across states in formulating and implementing privacy and security solutions. The project team has been working closely with Alaska and Oregon. Additionally, because of the state's participation on the Consumer Engagement and Standards Adoption Collaborative work groups, Washington has become well integrated with other states.

#### **4.1.32 West Virginia**

##### *Health IT/HIE Privacy and Security Landscape Before Privacy and Security Solutions Project*

The West Virginia Medical Institute (WVMI), the Quality Improvement Organization for the state, performed an environmental scan related to the status of health IT implementation at the end of 2005 as a deliverable for its contract with CMS. The scan revealed growing interest in health IT in West Virginia but little coordination between efforts. All major hospitals and physician associations were actively involved in encouraging the use of health IT. Highlights of the scan include the following:

- Seventeen critical access hospitals (CAH), 36 acute care hospitals, and 13 specialty hospitals (including psychiatric, ENT [ear, nose, and throat], and rehabilitation) were operating in West Virginia.
- Only a small number of hospitals—5 acute care and 1 CAH—had CPOE systems.
- Most hospitals, even CAH, provided physician practices access to lab results, and a smaller number provided access to radiology results.
- Only 6 acute care hospitals provided their on-campus practices with an EHR (no CAH had this capacity).
- No pay-for-performance initiatives were in place yet within the state.
- Primary care practices tended to be small. Less than 10% of them had implemented any form of EHR, and these practices used a broad variety of vendor products.
- Seven state-operated hospitals and clinics and 4 federally qualified health clinics were implementing VistA EHR.
- The Robert C. Byrd Rural Health Center at Marshall Medical School was piloting the Walter Reed HEALTHeFORCES software.

Charged by CMS to enhance the use of health IT through much of the health care provider continuum, WVMI developed relationships with nearly all health IT stakeholders in West Virginia. Working in collaboration with the West Virginia State Medical Association and the West Virginia Hospital Association, WVMI initiated the legal incorporation of the West Virginia eHealth Initiative (WVeHI), with these 3 groups as the first members of the WVeHI Executive Board. The steering committee of WVeHI included all of the major health IT stakeholders in the state with the exception of consumers. WVeHI was a subcontractor to

Accenture on the NHIN prototype contract and worked with Accenture to develop a regional health information network in West Virginia.

Senate Bill 170 was passed in March 2006 establishing the West Virginia Health Information Network (WVHIN) as a public-private partnership to promote the design, implementation, operation, and maintenance of a fully interoperable statewide network to facilitate the public and private use of health care information in the state.

### *Current Health IT/HIE Landscape*

Health IT and health information exchange in West Virginia continue to have strong momentum in West Virginia, including extensive support from the governor's office. Recent health IT and health information exchange activity in West Virginia includes the following:

- WVHIN will participate in the Nationwide Health Information Network trail implementations.
- Appalachian Regional Healthcare will deploy an EHR system to more than 190 employed and affiliated physicians in rural communities across eastern Kentucky and West Virginia.
- The William R. Sharpe Jr. Hospital is the first of 7 state-operated hospitals in West Virginia that has implemented Medsphere's OpenVista EHR platform. Clinicians now have the ability to retrieve patient records electronically.

The Privacy and Security Solutions project encouraged West Virginia to work across states in formulating and implementing privacy and security solutions. Through the regional and national meetings, the state team was introduced to other states working on the same issues. Through these contacts, West Virginia has been able to share information and documents with these other states, and is participating in the consumer education collaborative. West Virginia's in-state work on education has helped inform the collaborative's work.

Several health IT initiatives in West Virginia have been either directly or indirectly affected by the project. For instance, West Virginia has applied for a grant from the Federal Communications Commission, and WVHIN was recently awarded an NHIN trial implementations contract. The West Virginia team reported that the State Medical Association and the West Virginia Academy of Family Physicians have asked for background information on the Privacy and Security Solutions project and that more physicians have adopted, or plan to adopt, EHRs. Additionally, Marshall University is preparing to roll out an e-prescribing initiative.

### *Current Privacy and Security Landscape*

WVHIN acts as the governance body in West Virginia and has integrated the Privacy and Security Solutions project into the WVeHI Executive Board as part of a formal privacy governance structure.

In West Virginia, the Privacy and Security Solutions project provided an impetus to the introduction of enhanced privacy and security procedures across the legislative branch. The West Virginia legislature recently enacted 2 of the project's high-priority legislative proposals, including a bill to amend an existing state statute by providing greater flexibility in the disclosure of confidential mental health information. The project was also instrumental in introducing the state to a group of initiatives being sponsored in other states that focused on the privacy and security aspect of health information exchange.

In their findings from Phase I of the Privacy and Security Solutions project, the West Virginia project team recommended that West Virginia create additional opportunities to educate consumer stakeholder groups concerning health information exchange privacy and security concerns. West Virginia's population is dominated by a high percentage of low-income elderly, rural Medicare and Medicaid recipients with numerous chronic conditions that make them frequent users of health care. The West Virginia team thought it necessary to delve into how to work with this unique population, information that may not be obtained from other states with younger more urban residents.

The West Virginia team reported that the Privacy and Security Solutions project helped them to formulate their implementation plan into action and educate their consumers so that they can develop a sustainable plan for West Virginia's security and privacy concerns for the future. West Virginia intends to fully implement the plan in 2008, in conjunction with WVHIN and the multistate collaborative that is focusing on consumer education, outreach, and dissemination.

WVMI established a speakers' bureau and set up a series of presentations to a variety of consumer groups throughout West Virginia. West Virginia's original proposal stated that 15 educational presentations would be held throughout the state. However, demand for the presentations has been such that 17 have been completed in various geographic regions throughout the state and to varied consumer groups. Several more presentations are planned for December 2007. The consumer groups include seniors, chronic disease support groups, West Virginia businesses, health care trade organizations, consumer advocacy groups, and the Alzheimer's Association Annual Meeting. The presentations were approximately 1 hour, using a PowerPoint slide show with a 1-page handout as educational tools. The findings from the educational presentation discussion/question answer sessions were similar to the results of the focus groups and survey. All materials will be disseminated on WVHIN's website at [www.WVHIN.org](http://www.WVHIN.org) and on WVMI's website at [www.wvmi.org](http://www.wvmi.org). The materials will be shared with other state collaborative partners and key stakeholders in West Virginia.

Based on recommendations of the West Virginia project, the West Virginia legislature passed 2 bills during the last session. These include West Virginia HB 3184, a bill to amend an existing state statute by providing greater flexibility regarding the disclosure of

confidential mental health information, and West Virginia SB 1001, a bill to amend an existing state statute by adding a new section relating generally to the authorization of electronic prescribing.

The executive branch of West Virginia state government recently accepted a statement of 6 privacy principles that will be used to frame the discussion on privacy for health information exchange activity. In the near future, a set of security principles will be enacted. The knowledge base acquired through Privacy and Security Solutions project has also framed consumer education research and outreach activities. These experiences, in turn, will support developing consumer messaging that directly speaks to the concerns the public voiced about health information exchange and health IT.

#### **4.1.33 Wisconsin**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

In response to state and national health care goals, Wisconsin Governor Doyle issued Executive Order 129 on November 2, 2005, creating the Board on eHealth Care Quality and Patient Safety (also known as the eHealth Board) with the goal of developing a road map for statewide use of interoperable EHRs to improve patient care while protecting patient privacy. In March of 2006, the eHealth Board sponsored the state's proposal (developed by the Department of Health and Family Services [DHFS]) to participate in the Privacy and Security Solutions project. The eHealth Board serves as the steering committee for the Privacy and Security Solutions project in Wisconsin.

In December 2006, shortly after the initiation of the Privacy and Security Solutions project, the eHealth Board delivered the *eHealth Action Plan* to the governor. The plan helped to coordinate several independent activities that were currently under way in Wisconsin. Wisconsin's participation in the Privacy and Security Solutions project was instrumental in identifying and resolving privacy and security issues faced by each of these initiatives and to achieving a comprehensive statewide structure for health information exchange. Following is a list of the initiatives and entities that were active at the beginning of the project:

- The HIPAA Collaboration of Wisconsin (HIPAA COW), a nonprofit organization created by the major Wisconsin public and private health care organizations to assist covered entities, business associates, and other interested parties in implementing the practices required by HIPAA.
- The Madison Patient Safety Collaborative was formed to provide structure for area health care providers to work collaboratively to develop, share, and implement patient safety solutions. The collaborative was exploring the level of interest among its members for creating a RHIO for south central Wisconsin.
- The Wisconsin Medicaid program made an Internet query system available to emergency room (ER) physicians to track ER use by Medicaid recipients who are frequent users of ER care.

- Metastar, a nonprofit health care Quality Improvement Organization led the DOQ-IT project in Wisconsin.
- The Goal-Oriented Patient Privacy Preservation study funded through a grant from the National Science Foundation CyberTrust program to the University of Wisconsin's Computer Sciences Department
- The Wisconsin DHFS was awarded a Robert Wood Johnson Foundation InformationLinks grant to support the development of RHIOs in December 2005.
- The Rural Wisconsin Health Cooperative was awarded a planning grant by AHRQ to begin work on behalf of 19 health care organizations, both rural and urban, to improve the quality of care and efficiency of service delivery by leveraging health IT.
- The Wisconsin Health Information Exchange, a membership organization of health care entities, was designed to create, govern, and continuously improve regional exchange of health information.
- The Wisconsin Health Information Management Association (WHIMA) is a nonprofit organization providing leadership for the management of health records in Wisconsin had assembled a toolkit for members that references 31 sources of information on issues related to the privacy and confidentiality of patient health information.
- The Wisconsin Health Information Organization (WHIO) is a nonprofit organization established in August 2005 to create the state's largest warehouse of information on the cost and outcome of health care provided by hospitals and doctors.
- The Wisconsin Medical Society committed to active involvement in the design and implementation of quality improvement initiatives and is a founding member of WHIO, a participant in InformationLinks, and has passed a resolution calling for widespread adoption of EHRs.

### *Current Health IT/HIE Landscape*

Wisconsin's formal governance structure for health privacy and security is composed of the DHFS, which is assigned responsibility for health privacy by state statute, and Wisconsin's eHealth Board, which approves recommendations to change state statute before legislative changes are introduced. The chair of the eHealth Board is Secretary Kevin Hayden, of the Wisconsin DHFS. DHFS is the Privacy and Security Solutions project subcontractor in Wisconsin, and the eHealth Board serves as the project's steering committee. Additionally, the work groups for the Privacy and Security Solutions project (assessment, solutions, implementation, and legal) report directly to the eHealth Board. The chair of each of the project work group is a member of the eHealth Board and DHFS personnel are assigned to each of the work groups. Through this structure, the project has added momentum to several health IT and health information exchange initiatives in Wisconsin.

HIPAA COW is a strong force for advocating health privacy and security issues in the state. Wisconsin foresees cross-state collaboration projects, especially as electronic exchange across state lines becomes more of a reality. General discussions with Iowa and Minnesota have already taken place.

In December 2006, the eHealth Board published Wisconsin's Action Plan for Health Care Quality and Safety. The action plan includes an executive summary and reports from e-health advisory groups, including consumer interest, financing, governance, information exchange, and patient care. Ensuring broad stakeholder representation in these groups and on the eHealth Board is considered to be extremely important in Wisconsin's e-health efforts.

A report by the US Department of Health and Human Services' Office of Inspector General found that Wisconsin is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the Privacy and Security Solutions project are Florida, Iowa, Kansas, Louisiana, Mississippi, Vermont, and Wyoming.)

### *Current Privacy and Security Landscape*

Through the governance structure described above, the Privacy and Security Solutions project has stimulated the creation, advancement, or endorsement of health IT adoption and health information exchange within Wisconsin by

- identifying conditions of exchange (both in practice and in law) and better preparing the state for health information exchange by addressing barriers in a more timely fashion;
- providing the opportunity to create consensus among a broader group of stakeholders than would have been otherwise possible;
- providing the opportunity to broaden the breadth and depth of analysis on exchange of sensitive health privacy topics than would have been otherwise possible; and
- providing the opportunity to engage in conversations with neighboring states.

In Phase I of the Privacy and Security Solutions project, the Wisconsin project work groups found that barriers to health information exchange were driven by variation among Wisconsin's state privacy laws and variation between Wisconsin statute and federal HIPAA privacy regulations. To address the variation found, the Consumer Interests Advisory Group (CIAG), one of the 5 advisory groups of the WI eHealth Board, met in May to review findings and make recommendations on efforts for the rest of 2007. At this meeting, the CIAG recommended changes to Wisconsin Statute section § 51.30 (§ 51.30) to address issues related to exchange of health information for treatment purposes and changes to Wisconsin Statute chapter 146 to mirror HIPAA in specific areas.

Except under limited circumstances, § 51.30 provides protections for mental health, developmental disability, and alcohol and other drug abuse (AODA) treatment information. The statute prohibits the disclosure of this information to providers for treatment purposes

unless consent is obtained from the patient or their legally authorized representative. This consent requirement is more stringent than the HIPAA Privacy Rule and Wisconsin laws governing other types of health care information that permit disclosure of health care information for treatment purposes without patient consent.

In Phase I of the Privacy and Security Solutions project, the Wisconsin team found that many providers were confused regarding when the statute allows for the exchange of data for treatment purposes, causing the statute to be applied inconsistently. To further complicate matters, § 51.30 allows for protected information to be exchanged within the patient's health care entity, but not across health care entities. Therefore, if a patient were to visit a doctor outside of the primary health care entity, that doctor would not be aware of psychiatric medication prescribed to the patient, leading to potential adverse drug interactions. Exclusions such as this could be detrimental to the patient's health and care.

Over the past year, the CIAG and the Wisconsin Privacy and Security Solutions Project team have grappled with this variation in law in an effort to better understand the variation's effect on health information exchange. Following its discussion on the matter, the CIAG recommended changing § 51.30 to comport with HIPAA for treatment purposes. However, noting a lack of consensus and concern from interested parties, Wisconsin project members involved in the discussions proposed an alternative, broad-based, approach to further discuss the issue.

The § 51.30 Work Group was convened in August 2007 by the Wisconsin Privacy and Security Solutions project team and with the approval of the eHealth Board. This work group addresses issues related to the stringent consent requirements of § 51.30. The Wisconsin Privacy and Security Solutions project team reached out to its community stakeholders to assure a greater variety of stakeholder representation in the § 51.30 work group. Stakeholders included mental health advocates (including representatives from Disability Rights WI, Mental Health America of WI, NAMI WI, and WI DHFS personnel), AODA advocates and administrators, developmental disability advocates, the Mendota Mental Health Institute, the Central WI Center for the Developmentally Disabled, physicians, consumers, state and county government, payers, large provider systems, the WI Hospital Association, and the WI Medical Society. The enhanced stakeholder group provided a more comprehensive picture of the uses and impacts of changing § 51.30.

The § 51.30 work group held 5 in-person meetings lasting 3 hours and exchanged numerous e-mails and review material to further the work. Through this process, the § 51.30 work group was able to achieve a consensus-based recommendation that met the needs of all stakeholder groups participating in the work group and helped to reduce the barriers to the electronic exchange of treatment data. The work group's recommendation calls for the amendment of § 51.30 to allow easier access to health care information for treatment purposes while maintaining an adequate level of privacy and security. The §

51.30 work group recommends disclosure, without patient consent, of the following information contained in the § 51.30 treatment record to all treating providers with a need to know: name, address, date of birth, name of mental health provider(s), date of service(s), diagnosis, medication, allergies, other relevant demographic information, diagnostics such as labs, imaging, and EKGs (excluding psychiatric testing), and symptoms. The recommendation also removes the “related health care entity” clause from § 51.30(4)(b)8g and adds “diagnostics” and “symptoms” to the list of information exchangeable without patient consent. The § 51.30 work group reported that by removing the “related health care entity” clause, doctors in different health care entities would now be able to exchange data for the purposes of treatment without having to obtain additional consent from the patient.

Additionally, the recommendations highlight other topics related to § 51.30 that the workgroup identified as high-priority areas for future action and consideration. These areas include: clarification of who is considered a provider, liability and penalty for unauthorized disclosure, provider education, notification, and clarification of various terms and conditions not clearly defined in § 51.30.

Wisconsin’s Consumer Interests Advisory Group and Privacy and Security Solutions Project Implementation Work Group (IWG), in their examination of § 51.30, noted that changes to § 51.30 would impact mental health and developmental disability health care information, but not AODA information. As the more stringent law, the applicable sections of 42 C.F.R. pt. 2 would control AODA record information and override the proposed changes to § 51.30. Therefore, in keeping with 42 C.F.R. pt. 2, informed consent for AODA record information would still be required for provider to provider exchange for treatment purposes except in medical emergencies.

The Wisconsin project team also addressed Wisconsin Statute § 146, which governs general health care information. The HIPAA Privacy Rule affords many of the same privacy protections at the national level that § 146 affords Wisconsin citizens, with some variation. In its *Implementation Plan Report*, Wisconsin’s IWG proposed changes that would standardize current practices in Wisconsin and better align Wisconsin law with HIPAA.

During Phase I, the project team found 3 specific areas of § 146 that inhibited electronic exchange of health care information. The first topic is documentation. Currently, § 146 requires documentation of all disclosures (written or oral) with or without consent. This documentation becomes a legal part of the patient’s record. The requirement to record even oral disclosures makes this requirement very difficult for health care entities to follow. The proposed change to § 146 is to mirror 45 C.F.R. 164.528, which requires limited documentation of disclosures that enable the patient to determine who has accessed his/her health information and when.

The second topic addressed by the Wisconsin Privacy and Security Solutions Project team was related to redisclosure of data. Currently, § 146 requires that when information is disclosed without patient consent, the recipient must keep the information confidential and may not redisclose it. The project team found that this requirement was not in agreement with requirements found in § 51.30. The proposed change for redisclosure is to add language to § 146 that allows redisclosure with patient consent or where otherwise allowed by law. The proposed change would mirror language found in § 51.30.

The third topic addressed the disclosure of information to individuals involved in the care or treatment of the patient. Currently, § 146 requires patient consent to provide written or oral disclosures of health information to individuals involved in the care or treatment of the patient. The proposed change to § 146 is to allow oral disclosure to individuals involved in the care or treatment of the patient with patient agreement (not formal consent). The proposed changes would retain requirements for patient consent to disclose any copy of a patient's medical record.

A privacy consultant representing the Department of Health and Family Services met with stakeholders/stakeholder groups to discuss the proposed changes. Stakeholder responses were documented and a draft detailed summary and analysis of the responses was created. The concerns will be further evaluated, possibly resulting in modifications to the initial proposed changes. The Wisconsin Privacy and Security Solutions project team noted that the changes to the redisclosure piece of § 146 were not considered to be controversial and were agreed to by all stakeholders queried.

Part of Wisconsin's Phase II work involves clarification of 42 C.F.R. pt. 2 through a partnership with the Privacy and Security Solutions project team in Indiana and their multistate steering committee. As a supporting partner in this effort, Wisconsin's role is to assist Indiana in its efforts in considering the feasibility of implementing proposed changes, convening stakeholder groups and local experts as needed.

Throughout all phases of the Privacy and Security Solutions project, the Wisconsin team has emphasized the inclusion of interested stakeholders in the process. The eHealth Board as well as its 5 advisory councils are public-private partnerships comprised of state employees, health care providers, advocates, and consumers. The composition of the § 51.30 work group leaned heavily towards stakeholders and included mental health, AODA, and developmental disability advocates among others.

In this vein, the Wisconsin Privacy and Security Solutions Project team is planning a series of town hall meetings in 2008 that will educate the public on issues relating to privacy and security as well as the proposed changes to Wisconsin Statutes § 51.30 and § 146. The Wisconsin Privacy and Security Solutions project team began preparing for the town hall meetings during the July-December 2007 extension period. The governor's office became aware of the project team's efforts and asked to be involved in the process. In mid-January,

the Wisconsin Privacy and Security Solutions Project team and the governor's office will hold 2 pilot meetings with 30-40 attendees at each meeting. The purpose of these pilot meetings is to gauge interest in privacy and security and to develop the content for the town hall meetings. Four town hall meetings have been planned to occur throughout Wisconsin in February and March 2008. Through the involvement of the governor's office and the town hall meeting planning, the Wisconsin Privacy and Security Solutions project has gained momentum and visibility.

#### **4.1.34 Wyoming**

##### *Health IT/HIE Privacy and Security Landscape Before the Privacy and Security Solutions Project*

With a population of about 500,000 people spread over approximately 100,000 square miles, Wyoming is one of the most sparsely populated states in the nation. Access to needed medical services can be a significant challenge owing to great distances, geographic features such as mountains and range land, and a chronic shortage of most types of health care providers. Wyoming health care partners view electronic health information exchange as important technology to improve quality and access to health care and achieve such goals as fewer hospital admissions from the emergency department, fewer readmissions, reduction in medical errors, shortened length of stay at the hospital, enhanced revenue from proper coding, and reduction of duplicative tests. Collaborative health care partners have sought a statewide health IT program for Wyoming.

In 2003, the Wyoming legislature created the Wyoming Healthcare Commission (WHCC) to develop strategies to improve health care and reduce health care costs for Wyoming citizens. In 2004, the legislature passed Enrolled Act 31, directing WHCC to create an Information Technology Technical Management Subcommittee (IT2) to study and plan for a statewide interoperable health information exchange network by October 15, 2005. To help evaluate the feasibility of such an effort and develop a health IT plan for Wyoming, the state commissioned an assessment of Wyoming's electronic health information readiness and called for recommendations to increase the use of technology in accessing patient health information. This study (John Snow, Inc., 2006) described the state in the early stages of health IT adoption and development, both in the public sector and among private health care entities.

A number of health IT initiatives existed throughout Wyoming at the time the Privacy and Security Solutions project proposal was written, including the Indian Health Services initiative on the Wind River Indian Reservation, Wyoming Network for Telehealth, the Department of Veterans Affairs initiatives, and the DOQ-IT study.

On June 29, 2005, WHCC recommended to the governor and the legislature's Labor, Health, and Social Services Committee that Wyoming form a self-sustaining RHIO to facilitate an

intrastate, regional interstate, and national federal partnership for the rapid deployment of Wyoming's electronic health information infrastructure. In July 2005, more than 50 representatives of local, state, and federal government, medical care providers, and health care purchasers and payers gathered to discuss the development of a RHIO for Wyoming. On August 11, 2005, this RHIO was registered with the Wyoming secretary of state's office as the nonprofit Wyoming Health Information Organization (WyHIO). The WyHIO's mission is "to enhance access, quality, safety, and the efficiency of healthcare in Wyoming through the implementation of electronic information exchange and interoperability that is secure and confidential and utilizes technology that will assure interconnectivity within Wyoming and the rest of the nation" (Wyoming Health Information Organization, 2005).

### *Current Health IT/HIE Landscape*

The WyHIO is pursuing focused initiatives that will provide specific value to health care entities using a health IT network, including statewide electronic prescribing. This initiative involves developing several different objectives, including a continuity of care record creating a summary of patient health information that would be immediately available to providers; hospital portals to allow authorized, secure inquiry of hospital patient data; and development of a technology support organization to manage the network.

The WyHIO allows Wyoming to evaluate and endorse projects and processes that will integrate with state, regional, and national health IT efforts. Continuing coordination of initiatives will be an important part of developing the Wyoming health IT network.

Wyoming is still working toward the goal of establishing a statewide health IT program. To that end, the WHCC initiated the following projects in 2006:

- Indian Health Services initiative on Wind River Reservation
- Wyoming Network for Telehealth
- health IT initiatives within the Department of Veterans Affairs
- DOQ-IT project

Other initiatives are in the development stage, including an HIE Policy Coordinating Center, an HIE demonstration project, and initiatives that would work on developing sustainable support and researching legal harmonization within the state. There is also an initiative to develop a health IT commission within the state.

A report by the US Department of Health and Human Services' Office of Inspector General found that Wyoming is among only 12 states where Medicaid agencies have implemented health IT initiatives for Medicaid beneficiaries and participating providers (Department of Health and Human Services, Office of the Inspector General, 2007). These states are noted by federal officials as being among the first in a long-range national plan to improve the quality of health care and control spiraling costs by the year 2014. (Other states in the

Privacy and Security Solutions project are Florida, Iowa, Kansas, Louisiana, Mississippi, Vermont, and Wisconsin.)

In June 2007, Wyoming Governor Dave Freudenthal appointed several individuals to a Health IT Task Force. The goal of this group was to make recommendations relating to health IT for the upcoming legislative session, and there are no plans to continue the task force beyond this original commission at this time. The primary expected outcome of the task force is the designation of the WyHIO as the recognized policy organization for health information exchange within the state. The WyHIO is largely an oversight body and does not currently engage in exchanging data. However, several regional pilot projects are being investigated.

Of particular interest to stakeholders in Wyoming is a need to collaborate across states in formulating and implementing privacy and security solutions, because many consumers seek health care outside of the state. This is attributed to the present nature of Wyoming's health care system. However, at this stage stakeholders are focusing on developing resources within the state. They have been discussing opportunities to develop intrastate exchange with Colorado, Utah, and Mississippi, but they recognize that Wyoming needs to advance information exchange within the state first for larger efforts to be effective.

#### *Current Privacy and Security Landscape*

The Privacy and Security Solutions project led state team members to identify or interact with stakeholders who might not otherwise have become involved. This project supported outreach in communities outside major cities to encourage their involvement. Stakeholders from these less populated areas of the state are now key players in the formulation of health IT and health information exchange. For example, legislators from outlying areas, consumers, and small physician offices have helped raise awareness that this issue affects everyone, even outside the major urban areas. They worked with individuals in diverse groups, ranging from rural home health care services to the governor's health policy advisor.

The WyHIO will take over responsibilities of the Wyoming project's Policy Center and will be a resource for disseminating information about health IT in the state. The Privacy and Security Solutions project enabled discussion of health IT and health information exchange issues within a context that has brought privacy and security issues to the forefront. The creation of Governor Freudenthal's Health IT Task Force can be attributed, at least in part, to the many discussions that occurred between the project team and the governor's health policy advisor on privacy and security issues.

The Privacy and Security Solutions project has raised major privacy and security issues for the Southeast Wyoming TeleHealth network, which includes 6 hospitals in southeast Wyoming. This outcome has highlighted privacy and security issues common to both

telehealth and electronic health information exchange, and has identified efficiencies in developing common policy and practices for both exchange media. One example is the need for policies (such as consent protocols) and procedures to ensure privacy when clinical information is exchanged via the Telehealth network. Because the network is used primarily for educational purposes, the project highlighted these concerns. When the governor's office designates WyHIO as the health information exchange coordinating body, it is expected that the WyHIO will have a more specific mandate for maintaining privacy and security in health information exchange.

Finally, the Privacy and Security Solutions project team in Wyoming has identified the need for working across state lines and accelerating the formulation and implementation of privacy and security solutions for interstate exchange. Because of limitations in the state's health care system, many in Wyoming frequently seek help from providers based outside the state boundaries.

## 4.2 Impact in Nonparticipating States

Of the 9 states that applied for, but did not receive funding in Phase I of the project, 7 (Georgia, Maryland, Missouri, Nebraska, South Dakota, Tennessee, and Texas) have joined the project in Phase II to participate in the collaborative work groups. Additionally, 3 of these states have conducted significant privacy and security-related activities during Phases I and II of the project and have identified measurable impacts to privacy and security solutions as a result of this work.

Nebraska utilized the Privacy and Security Solutions project methodology and carried out the project within their state using other available sources of funding and the original group of diverse stakeholders they had assembled to prepare their initial proposal. They published a final report of their Phase I work,<sup>10</sup> and decided to focus on outreach and education for consumers and providers, and aligning state laws as their Phase II implementation activities. Based on discussions with the state project director, the following impacts of the project were noted:

- Passage of state legislation in February 2007, which allowed the 2-way exchange of electronic medical information and clarified rights and protections associated with such exchanges (LB 185 Section 71-5185).
- Creation of an integrating body (eHealth Council<sup>11</sup>) with 25 members—4 of whom are representatives from the Privacy and Security Solutions project.
- Creation of a clearinghouse of information related to what is happening nationally and internationally in health information exchange, with an overall intent to promote the idea that information exchange at every level is critical.

---

<sup>10</sup> [www.nitc.ne.gov](http://www.nitc.ne.gov)

<sup>11</sup> <http://www.nitc.ne.gov/eHealth/HealthCounciloverview.pdf>

- Plans to implement the tools developed through the Consumer Education and Engagement and Provider Education Collaborative work groups within the state.
- Participation in the Standards Policy Adoption Collaborative Work Group.
- Creation of an eHealth Coordinator position within the state Department of Health and Human Services.
- Application of business policy and procedure standards related to privacy and security to the 3 RHIOs operating within the state [Nebraska Health Information Initiative; Western Nebraska Health Information Exchange; and the Medicare Rural Hospital Flexibility Program Critical Area Hospitals (Hebron and Lincoln Hospitals)].
- Hospital Flexibility Program Critical Area Hospitals (FLEX CAH) (Hebron and Lincoln hospitals) for use as a model for cross-state exchange.

Tennessee also utilized the Privacy and Security Solutions project methodology to implement the project using state funding for stakeholders with whom they already had established relationships. The project methodology provided the tools that maximized the productivity of the discussions about privacy and security solutions. The project focused on conducting a legal and legislative review, which was published and circulated among members of the General Assembly. Based on discussions with the state project director, the following impacts of the project were noted:

- passage of state legislation in May 2007, which allowed for laboratories to become trusted entities and permitted them to participate in health information exchange (Public Chapter No. 301);
- publication of the legislative review, which has become a key tool for formulating future legislation related to privacy and security solutions;
- provision of policy recommendations related to privacy and security for the 2 RHIOs within the state—Mid-South eHealth Alliance and Carespark; and
- provision of policy recommendations related to privacy and security for the 2 HIEs within the state—the Innovation Valley Health Information Network and Shared Health—that in turn are providing the developing exchanges with lessons learned and information on their successes and failures.

Maryland developed a parallel project to the Privacy and Security Solutions project, funded with internal state monies. They secured the support of the governor, set up a project center, and conducted the project modeled after the Privacy and Security Solutions project. Currently, the Solutions Work Group is meeting and developing implementation plans that will be ready in January 2008. Based on discussions with the state project director, the following impacts of the project were noted:

- Established a Request for Applications process to design and construct a statewide health information exchange funded at a level of \$750000 for planning and \$10000000 for construction.
- Founded the Statewide Area HIE (SAHIE) harmonization project with 40 hospitals in the state that will be exchanging clinical health information.

- Created a reference guide (as part of SAHIE) for service area health information exchange at hospitals that includes technology and policy (privacy and security) recommendations.
- Created a Task Force (Task Force to Study Electronic Health Records) through the governor's office that will make a series of recommendations about EHR adoption and electronic health information exchange. The report of these recommendations is in final editing stages at this writing.
- Passed state legislation in April 2007 establishing a health information exchange pilot project (House Bill 979).

Of the states and territories that did not apply for funding in Phase I, 4 states and 1 territory (District of Columbia, Guam, Idaho, North Dakota, and Virginia) have established and maintained active contact with the project, including attendance at 1 or more of the regional and national meetings.



## 5. CONCLUSIONS

This report has described the progress that the state teams have made over the past 18 months toward meeting the Privacy and Security Project's goals, which include

- Assess variations in organization-level business policies, practices, and state laws that affect health information exchange;
- Identify and propose practical solutions, while preserving the privacy and security requirements in applicable federal and state laws, and;
- Develop detailed plans to implement solutions.

All of the work conducted by the 34 state teams since their formation in late spring 2006 and all of the work conducted by states independent of the project has been guided by their dedication to ensuring that, as the health care system takes advantage of the benefits of health information technology (health IT) and health information exchange, the privacy and security of health information will be protected.

The teams identified, and are now acting to reduce, sources of variation. They are working together to create common policies to permit private and secure nationwide electronic health information exchange. They are actively educating and engaging stakeholders within their individual states, and have laid the groundwork for an enduring statewide constituency through which to work to achieve consensus on the implementation of new solutions. The infrastructure is now in place to position state teams to work together toward harmonizing privacy practices, policies, and laws both within and across states lines. They have also built in their communities a knowledge base about privacy and security issues in electronic health information exchange that endures to inform future health information exchange activities. The next steps for the state teams include accelerating the implementation of solutions by working in multistate collaboratives, developing dissemination pathways to achieve widespread adoption, and coordinating with the other national initiatives.



## 6. REFERENCES

- Agency for Healthcare Research and Quality. *Evolution of State Health Information Exchange: A Study of Vision, Strategy and Progress*. Rockville, MD: Agency for Healthcare Research and Quality; 2006. AHRQ publication 06-0057.
- Connecting for Health. *Model Privacy Policies and Procedures for Health Information Exchange*; 2006.
- Department of Health and Human Services, Office of the Inspector General. *State Medicaid Agencies' Initiatives On Health Information Technology And Health Information Exchange*. <http://oig.hhs.gov/oei/reports/oei-02-06-00270.pdf>. August 2007, Accessed December 2, 2007.
- Dimitropoulos L. *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variations and Analysis of Solutions*. Chicago, IL: RTI International; 2007.
- EHealth Initiative. *Emerging Trends and Issues in Health Information Exchange: Selected Findings from eHealth Initiative Foundation's Second Annual Survey of State, Regional and Community-Based Health Information Exchange Initiatives and Organization*. Washington, DC: eHealth Initiative; 2005.
- EHealth Initiative. *Improving the Quality of Healthcare Through Health Information Exchange: Selected Findings from eHealth Initiative's Third Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels*. <http://toolkit.ehealthinitiative.org/assets/Documents/eHI2006HIESurveyReportFinal09.25.06.pdf>. Published September 25, 2006. Accessed November 14, 2007.
- EHealth Initiative. *Status of Statewide HIE Initiatives in Mississippi*. <http://ccbh.ehealthinitiative.org/communities/community.aspx?Section=288&Category=440&Document=1075>. Accessed November 14, 2007.
- Foundation of Research and Education. *Development of State Level Health Information Exchange Initiatives: Final Report—Extension Tasks*. Chicago, IL: American Health Information Management Association; 2007a.
- Foundation of Research and Education. *State Level Health Information Exchange: Roles in Ensuring Governance and Advancing Interoperability—Preliminary Report*. Chicago, IL: American Health Information Management Association; 2007b.
- Huang J. Health records could soon be online in state. *Kennebec Journal*. <http://kennebecjournal.mainetoday.com/news/local/3983829.html>. June 9, 2007. Accessed November 14, 2007.
- Iowa HIT Initiative. *Health Information Technology Adoption in Physician Offices, a Summary of Survey Findings in Iowa*. [http://www.iowamedical.org/articles/012507\\_HIT\\_Survey\\_Summary\\_of\\_Findings\\_Final.pdf](http://www.iowamedical.org/articles/012507_HIT_Survey_Summary_of_Findings_Final.pdf). Accessed November 14, 2007.

John Snow, Inc. Final Report to the Wyoming Healthcare Commission, Information Technology Technical Management Subcommittee on Developing a Wyoming Health Records Network. 2006.

[http://www.wyominghealthcarecommission.org/images/reports/11-16-07EHR\\_study.pdf](http://www.wyominghealthcarecommission.org/images/reports/11-16-07EHR_study.pdf). Accessed November 14, 2007.

Michigan Health Information Network. *Conduit to Care: Michigan's e-Health Initiative*.

[http://www.michigan.gov/documents/mihin/MIHIN\\_Report\\_Compress\\_v2\\_180321\\_7.pdf](http://www.michigan.gov/documents/mihin/MIHIN_Report_Compress_v2_180321_7.pdf). Published December 2006. Accessed November 14, 2007.

National Conference of State Legislatures website. 2007 Enacted Legislation on Health Information Technology.

<http://www.ncsl.org/programs/health/forum/hitch/enacted.htm>. Updated December 19, 2007. Accessed December 20, 2007.

National Conference of State Legislatures website. Health Information Technology Champions (HITCh). <http://www.ncsl.org/programs/health/forum/hitch/>. Updated October 29, 2007. Accessed November 14, 2007.

National Governors Association website. State Alliance for e-Health.

<http://www.nga.org/portal/site/nga/menuitem.1f41d49be2d3d33eacdcbbeb501010a0/?vgnnextoid=5066b5bd2b991110VgnVCM1000001a01010aRCRD>. Accessed November 14, 2007.

Remal G. Medical records moving online. *Morning Sentinel*.

<http://morningsentinel.maintoday.com/news/local/3812316.html>. April 15, 2007. Accessed November 14, 2007.

Vermont Information Technology Leaders, Inc, website. <http://www.vitl.net/>. Accessed November 14, 2007.

Wyoming Health Information Organization website. Mission Statement. 2005

<http://wyhio.org/2.html>. Accessed November 14, 2007.

## APPENDIX A: GLOSSARY OF ACRONYMS

This list is intended to serve as a quick reference for individuals working on health information exchange projects.

ACLU	American Civil Liberties Union
AFHCAN	Alaska Federal Health Care Access Network
AFMC	Arkansas Foundation for Medical Care
AHCA	Agency for Health Care Authority
AHCCCS	Arizona Health Care Cost Containment System
AHEDD	Automated Hospital Emergency Department Data
AHIC	American Health Information Community
AHIMA	American Health Information Management Association
AHRQ	Agency for Healthcare Research and Quality
AMIA	American Medical Informatics Association
AODA	alcohol and other drug abuse
BHIS	Behavioral Health Information System
CAH	critical access hospital
CaIPSAB	California Privacy and Security Advisory Board
CaIRHIO	California Regional Health Information Organization
CCIS	Chronic Care Information System
CCR	continuity of care record
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CHFS	Cabinet for Health and Family Services
CHI	Colorado Health Institute
CHIC	Community Health Information Collaborative
CHIME	Connecticut Health Information Management and Exchange Program
CHIN	Community Health Information Network

CHITA	Community Health Information Technology Alliance
CIPA	Consortium of Independent Physician Associations
CO EKG	Colorado EKG Repository
COHIE	Colorado Health Information Exchange
CORHIO	Colorado Regional Health Information Organization
CPOE	computerized physician order entry
CVD	cardiovascular disease
DHFS	Department of Health and Family Services
DHH	Department of Health and Hospitals (Louisiana)
DHHS	Department of Health and Human Services
DOBI	Department of Banking and Insurance
DOQ-IT	Doctor's Office Quality-Information Technology
ECAPS	Electronic Communication Across Provider Setting
EDI	Electronic Data Exchange
EHR	electronic health record
EHRIS	electronic health record system
ePPIK	e-Prescribing Partnerships in Kentucky
ER	emergency room
FHIN	Florida Health Information Network
FORE/AHIMA	Foundation of Research and Education of the American Health Information Management Association
FQHC	Federally Qualified Health Center
HCA	Health Care Authority
HCRP	Health Care Reform Panel (Louisiana)
HEAL-NY	Health Care Efficiency and Affordability Law for New Yorkers
HEALTH	Rhode Island Department of Health
HIE	health information exchange

HII	health information infrastructure
HIIAB	Health Information Infrastructure Advisory Board
HIIAC	Health Information Infrastructure Advisory Committee
HIMSS	Health Information and Management Systems Society
HINT	Healthcare Information Networks and Technology
HIPAA	Health Insurance Portability and Accountability Act
HIPAA COW	HIPAA Collaboration of Wisconsin
HISB	Health Information Standards Board
HIS/EMR	Hospital Information System/Electronic Medical Record
HISPC	Health Information Security and Privacy Collaboration
HIT	health information technology
HITCh	Health Information Technology Champions
HITSP	Health Information Technology Standards Panel
HPIO	Health Policy Institute of Ohio
HRSA	Health Resources and Services Administration
IDN	integrated delivery networks
IHIE	Indiana Health Information Exchange
IHIS	Integrated Health Information System
ILHIN	Illinois Health Information Network
INPC	Indiana Network for Patient Care
IPA	independent practice association
IQH	Information & Quality Healthcare
ISDH	Indiana State Department of Health
IT	information technology
KDHE	Kansas Department of Health and Environment
Ke-HN	Kentucky e-Health Network
K-HIP	Kentucky Health Information Partnership

KPHII	Kentucky Public Health Information Interchange
KU-CHI	University of Kansas Center for Healthcare Informatics
KUCTT	Kansas University Center for TeleMedicine and TeleHealth
LCF	Lovelace Clinic Foundation
LouHIE	Louisville Health Information Exchange
LWG	Legal Work Group
MAeHC	Massachusetts e-Health Collaborative
MA-SHARE	Massachusetts Simplifying Healthcare among Regional Entities
MCIR	Michigan Childhood Immunization Registry
MDCH	Michigan Department of Community Health
MDIT	Michigan Department of Information Technology
MDSS	Michigan Disease Surveillance System
MHDC	Massachusetts Health Data Consortium
MHIN	Michigan Health Information Network
MHINT	Maine Health Information Network Technology
MN-PHIN	Minnesota Public Health Information Network
NC DETECT	North Carolina Disease Event Tracking and Epidemiologic Collection Tool
NCEDD	North Carolina Emergency Department Database
NCHES	North Carolina Hospital Emergency Surveillance System
NCHICA	North Carolina Healthcare Information and Communication Alliance
NCSL	National Conference of State Legislatures
NGA	National Governors Association
NHIN	Nationwide Health Information Network
NIPFC	Northern Illinois Physicians for Connectivity
NMHIC	New Mexico Health Information Collaborative
NMHS	North Mississippi Health Services
NMMRA	New Mexico Medical Review Association

NYSDOH	New York State Department of Health
OFMQ	Oklahoma Foundation for Medical Quality
OHIE	Office of Health Information Exchange
OHII	Oregon Health Information Infrastructure
ONC	Office of the National Coordinator for Health Information Technology
OSEEGIB	Oklahoma State and Education Employees Group Insurance Board
PAiRS	Provider Access to Immunization Registry Securely
PDA	personal digital assistant
PHESS	Public Health Electronic Surveillance System
PHIN	Public Health Information Network
PHIX	Public Health eXchange (Kansas)
POL	Patient Online
PRDH	Puerto Rico Department of Health
RFP	request for proposal
RHIO	regional health information organization
RIQI	Rhode Island Quality Institute
RMRS	Regenstrief Medical Record System
SAHIE	Southern Arizona Health Information Exchange
SMUC	South Mississippi Urgent Care
SPTC	Security and Privacy Technical Committee
TCS	transaction and code set
UHIN	Utah Health Information Network
UMMC	University of Mississippi Medical Center
UNIFY	Utah Network for Electronic Public Health Information
VITL	Vermont Information Technology Leaders
WHCC	Wyoming Healthcare Commission
WHIO	Wisconsin Health Information Organization

WVeHI	West Virginia eHealth Initiative
WVHIN	West Virginia Health Information Network
WVMI	West Virginia Medical Institute
WyHIO	Wyoming Health Information Organization