June 30, 2007

Privacy and Security Solutions for Interoperable Health Information Exchange

Final Implementation Plans Executive Summary

Prepared for

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

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

Prepared by

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

Contract Number 290-05-0015
RTI Project Number 0209825.000.008

RTI Project Number 0209825.000.008

Privacy and Security Solutions for Interoperable Health Information Exchange

Final Implementation Plans Executive Summary

June 30, 2007

Prepared for

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

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

Prepared by

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

EXECUTIVE SUMMARY

This report is a summary of the 34 final Implementation Plans (IPs) that were drafted by the state project teams[1] under RTI International's contract with the Agency for Healthcare Research and Quality (AHRQ). The contract, entitled Privacy and Security Solutions for Interoperable Health Information Exchange, is jointly managed by AHRQ and the Office of the National Coordinator for Health Information Technology. The following summary report provides a glimpse into the activities that the 33 states and 1 territory that form the Health Information Security and Privacy Collaboration plan to implement in their states over the next 12 to 18 months.

Background

The IPs serve as both the culmination of prior work on the project and as practical tools for sustaining the development of privacy and security solutions that enable the electronic exchange of health information. To produce these plans, the state project teams followed a process that encouraged sharing observations, ideas, and concerns among an array of stakeholders including consumers, providers, insurers, state agencies, and others involved in health information exchange. The process began with the assessment of variations in business practices related to interorganizational exchange, the identification of barriers to electronic exchange, and the proposal of solutions to barriers that both enable the electronic exchange and maintain the privacy and security of health information.

The IPs summarized in this report are intended to be actionable documents that will guide the development and adoption of a framework for privacy and security for electronic health information exchange. The project teams in each state prepared both short- and long-term plans to protect privacy and security. Many of the plans mention uncertainty about funding for the implementation plans as a constraint in considering scope and schedule of the plans. Some plans included securing funding as a critical part of the plan.

Many of the IPs noted difficulty in considering privacy and security solutions in the absence of a practical model of how exchange might occur and where in the process safeguards can be put into place. Limitations also included interdependencies with national-level issues that remain to be resolved or addressed, and state and regional uncertainties with the legislative process needed to make changes or modifications to existing laws.

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

Implementing State-level Solutions

Implementing Leadership and Governance Solutions

In Section 4.1 we describe the state project teams' proposed approaches to leadership and governance of privacy and security activities moving forward. Fourteen of the 34 state project teams proposed the need for an oversight body. Eleven state teams proposed creating a new oversight body to lead and promote electronic health information exchange activities within the state, including implementing solutions and carrying on work done by the state project teams; issuing policy, technical, and/or legal guidance; and promoting interoperability. Teams proposed that this body could derive from a legislative or executive mandate.

In addition to the need for oversight, state project teams also planned to implement governance structures that include stakeholder work groups including legal and technical groups that would offer leadership and guidance as solutions are vetted and implemented. In addition to providing leadership and guidance, tasks assigned to the governing committees also included promoting the adoption and use of electronic health records (EHRs) and best practices to small and rural providers within the state.

The majority of state project teams proposing leadership and governance structures thought that this was feasible. Although the state teams were generally optimistic with respect to implementation, 13 state teams raised funding as the most likely barrier to success. Staffing and government support were the next most frequently cited barriers to implementation. State project teams where electronic health information exchange efforts were just beginning noted that they were eager to access the expertise available from states that are more advanced in setting up their efforts.

Implementing Practice and Policy Solutions

A majority of solutions state project teams put forward were multifaceted and most had a policy or practice component. For example, although approaches to obtaining and documenting patient consent and authorization included technology and legal components, there was widespread agreement about the need for common understanding on the critical elements that comprise patient consent and the need for a universal consent form. A number of states also noted that those policies will need to address consent management in emergency situations and for specially protected information.

Policy development was also proposed to reduce variation associated with the interpretation and application of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Many state project teams proposed plans to draft policy manuals and to provide training and policy guidance and education. One state proposed working with professional associations within the state to help develop consistent definitions and interpretations of terms and concepts related to the HIPAA Rules.

Several states proposed addressing the variation related to exchange of specially protected health information, which generally includes alcohol and drug abuse, mental health information, and human immunodeficiency virus/acquired immunodeficiency syndrome (HIV/AIDS) status, with policy solutions rather than making recommendations for federal action. Ten state project teams included policy solutions for exchanging specially protected health information.

Six state teams proposed the use of some type of model documents. Three state project teams planned to draft language for business associate agreements (BAAs),[2] to be used by HIPAA-covered entities within the state. One of these 3 state project teams intended to include education regarding model BAAs. Two additional state project teams made general reference to drafting standardized forms or policies, but did not develop these plans in greater detail.

Three state project teams addressed the issue of exchanging Medicaid data, with 2 state teams outlining implementation plans to do so. One state intended to establish policies to facilitate the flow of information between Medicaid and non-Medicaid providers. Another state proposed creating minimum security standards for sharing Medicaid data, implemented through contractual agreements.

Two state project teams raised the issue of exchanging information with public health authorities, although the plans were not fully developed. One state project team noted the value of law enforcement officials in emergency situations and raised the issue of data exchange with law enforcement. The team planned to offer targeted training programs for law enforcement officials including judges and to develop model protocols for information exchange by conferring with state agencies, the attorney general's office, and police on the design of the protocol. The state project teams noted that funding and stakeholder and consumer engagement were likely to be the biggest barriers to implementing policy solutions. Other potential barriers included resistance to change among health care staff and lack of political support.

Implementing Legal and Regulatory Solutions

Three state project teams included plans for updating state law to apply to electronic health information exchange. These ranged from broad unspecified plans to plans with a narrow

[2] The states generally used the term *business associate agreement* instead of the regulatory term *business associate contract or arrangement.* Either term is acceptable, but the agreement must be in some form of legally enforceable vehicle, such as a contract, or in the intra-governmental context, a memorandum of understanding. The HIPAA Privacy and Security Rules require covered entities to document satisfactory assurance that their business associate will safeguard health information through a written contract or other written agreement or arrangement. The rules have specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memorandums of understanding between agencies. Thus, the term *business associate agreement (BAA)* encompasses both contracts and other arrangements and this term is used in the summary above.

focus such as planning to update a law that requires wet signatures to accommodate electronic signatures when prescribing medications.

Proposed amendments to state law fell into 3 broad categories: amending state law to mirror federal law, amending state law to remedy state-specific concerns, and amending or drafting new state law to address consistency issues more broadly. Five state project teams drafted plans to align state law with federal law, usually HIPAA. Two teams made general reference to federal law, 1 explicitly referenced HIPAA, and the other 2 planned to incorporate the HIPAA Privacy Rule treatment, payment, and health care operations exemption from patient authorization into state law. State-specific concerns were related to specific language (or lack thereof) in state law. Four state project teams drafted language that could be used to amend state law related to consent, interactions between Medicaid and non-Medicaid providers, treatment, electronic health information exchange and minors, and specially protected information, including genetic testing results. Three project teams planned to amend state law to correct inconsistencies in definitions of terms and between state regulations governing the exchange of general health information and specially protected information.

Eleven teams' plans included recommendations for new legislation and 3 teams planned to draft new legislation, but were still in the process of examining the need for legislation in a number of areas. One team was unable to locate any state law that applied to electronic exchange and planned to form a committee to draft foundational laws and regulations.

The remaining legal and regulatory solutions fell into 2 general categories: consolidating or centralizing state laws and regulations, and considerations of the Physician Self-Referral Law and the Healthcare Antikickback Law (commonly referred to as the Stark and Antikickback Laws). Three state project teams planned to consolidate their state laws and regulations governing privacy and security. It was thought that collocating the various pieces of applicable legislation would facilitate legal analyses and reduce variation in business practices.

Two state project teams planned to resolve issues related to the Stark and Antikickback Laws. The Stark and Antikickback Laws prohibit physicians from receiving compensation, including nonmonetary compensation, for referrals of Medicare and Medicaid patients. In 2006, the Department of Health and Human Services (HHS) announced new regulations allowing exceptions for the donation of health information technology (HIT) equipment to facilitate adoption of HIT and EHRs. Although the state project teams did not fully develop their IPs for addressing these issues, they planned to do so in subsequent work.

State project teams identified a number of potential barriers to implementing regulatory solutions; the most frequently cited was lack of stakeholder support. The need to have full stakeholder support for any legislative change was recognized, although plans to gain that support were not fully formulated. One state anticipated resistance to their proposed

legislative amendment and included other options for amending state law, as well as an analysis of the risks and benefits of choosing other solutions.

Other commonly cited barriers included those related to the legislative process. Three states have legislatures that meet infrequently and/or for short periods of time. The compressed time frame of these legislative sessions makes it difficult to pass legislation that does not have substantial support from the outset. While some states were confident that they would receive support from legislators, 2 state teams expressed doubts about their ability to find sponsors for their legislation or to achieve consensus with those sponsors.

Implementing Technology and Standards Solutions

The majority of technology solutions focused on methods for patient and provider identification, user and entity authentication, authorization, and access controls. Several state project teams focused on developing a centralized provider directory to authenticate and authorize providers. State project teams also proposed using a master patient index and a provider identification management system to function within their HIE or regional health information organization. Other state project teams proposed probabilistic matching algorithms to match patients with their records. Ten of the state project teams included IPs related to user and entity authentication. Several state project teams studied biometrics and other authentication tools. One state planned to develop a personalized health smart card that individuals can carry. Another state was undertaking a pilot project to automate the flow of laboratory orders and results among the major laboratories servicing the state and health care providers. This was chosen as the vehicle for centralizing and sharing authentication services as well as implementing interorganizational secure messaging.

Eighteen of the state project teams planned to implement solutions related to information authorization and access controls to ensure access to data, people, or software programs that have been granted access rights. The plans ranged from developing role-based access standards that account for physicians' on-call coverage and emergency roles to implementing various authentication technologies. Many of the state project teams tackled the issues related to authentication, authorization, access, and audit as a group (ie, the 4 A's). The state project teams formed subgroups to research specific technology and process solutions using various exchange models including centralized, federated, and hybrid. Other states defined procedures and processes. One state project team is developing a consensus model document of policies and procedures based on the provisions of the HIPAA Rules. Another state project team drafted 19 principles or best practices to guide their implementation. Specific technology solutions proposed for implementation included digital signatures, digital certificates, biometrics, and USB and card swipe technologies. Several state project teams were developing software tools to assist in specifying *minimum necessary* information and specially protected health information. Seven state project teams focused on information audits that record and monitor the

activity of health information systems; most of the teams were planning to adopt industry standards, but other teams planned to develop a framework for what standards need to be reviewed and how to identify best practices.

Five state project teams planned to implement or strengthen information transmission security or exchange protocols for information exchanged over an electronic communications network. All of these teams will focus on the design and implementation of technical solutions for expanded data exchange services, and several state project teams will draft rules to govern how personal health information can be transmitted. One state project team was specifically examining encryption as a technical solution and planned to use their newborn screening program as a test case for implementing the new rules. Another state project team will require that any patient information being transmitted on external networks go through a virtual private network connection between client and server or network to network.

Five of the state project teams planned to implement broad information security standards and best practices. State project teams in the early planning stages for electronic health information exchange were working to develop vocabulary, data, and messaging standards while other state project teams planned to examine security standards in all 9 domains. Typical of the more comprehensive approach was the plan to form an information technology security committee to identify and establish a wide range of security standards for entities participating in an HIE that will initially focus on established security protocols, organizational standards, and minimum standards for exchange. Later work will involve testing and recommending common standards and protocols in conjunction with privacy policies for all areas of security. Another state project team planning a comprehensive approach planned to establish data element standards and create a best practices repository.

Implementing Education and Outreach Solutions

The majority of the states proposed some form of informational group meeting to share information about electronic health information exchange with consumers. The goal of the sessions is twofold: to educate consumers on the secure exchange of electronic health information and to solicit input regarding the implementation plans and process. In addition to the informational meetings, some states proposed utilizing a secure website to keep consumers engaged and updated. Several states also planned to create consumer advisory committees as a way to maintain consumer engagement.

Consumer education and engagement aims to address to 3 major issues: First, consumers are often not aware of their rights and responsibilities with respect to their health care records. Second, consumers may not be aware of the benefits of electronic health information exchange and EHRs. Finally, because of the lack of information, consumers may

mistrust HIEs and EHRs. As one state noted, "The cumulative differences in knowledge among consumers and health care industry staff naturally leads to mistrust and negatively affects consumers' confidence for participation in electronic health information exchange." Another observed:

> Patients and consumers are generally not aware of the privacy protections and rights they enjoy under the HIPAA Rules and state law. Because of this, many patients and consumers retain an unnecessarily high level of distrust regarding the storage and communication of their health care information when it is in electronic form. This high level of public distrust may threaten to delay or derail the transition of the health care delivery system into the information age.

Sixteen state teams included IPs for engaging with or educating consumers. These efforts included community forums, focus groups, pamphlets and other literature, and a website with frequently asked questions and other resources. Other options include television and radio campaigns and collaboration with consumer groups to raise awareness about the benefits of electronic health information exchange.

In addition to reaching out to consumers, state teams also planned outreach and educational efforts for providers. States identified different levels of knowledge among health care industry stakeholders about privacy and security requirements for electronic health information exchange. The purpose for the provider education plans is to reduce variations due to incorrect or incomplete understanding of relevant state and federal law. Provider education may also reduce liability concerns and facilitate exchange if providers are more confident in their compliance with state and federal law. Twelve state teams outlined education efforts for providers, with 5 of these functioning as components of broader educational efforts that include education and outreach for consumers and others, such as payers and employers. In addition to general awareness about electronic health information exchange and HIT, state teams also sought to raise awareness about specific issues. Three states proposed educational efforts relevant to newly passed or anticipated legislation that could change the way providers exchange information.

In addition to patients and providers, almost all of the state teams proposed plans for informational sessions tailored toward legislators and government leaders to garner support and funds for initiatives although the teams often did not include details on implementation with the exception of 1 state team that plans to hold a statewide health information network summit to share technological solutions to the privacy and security barriers identified in their state.

Two other groups that state teams identified as targets for educational efforts included public health and law enforcement officials. These individuals frequently need access to personal health information in order to conduct disease surveillance and investigation in the case of public health, and to assist in emergency care of a patient or to conduct criminal

investigations and prosecutions in the case of law enforcement. Three state teams planned educational programs for law enforcement officials. Two have already had success in working with the officers, and 1 includes relevant training for members of the service academy. One state planned to educate public health officials about their role in electronic health information exchange, but did not offer details. Finally, 1 state has included public health from the inception of their project, and has integrated a public health perspective into their entire planning process.

State teams felt that it was feasible to implement education and outreach programs. Although such programs may be costly, there are established frameworks for educating consumers and providers. In addition, the fact that many state teams feel that such education is critical to the success of electronic health information exchange and HIT makes these programs a priority.

Although the state teams believe that educational solutions are feasible, they do recognize that they will require special expertise in executing the education and outreach campaigns and therefore often listed the need to identify and hire a marketing or communication consultant to develop effective consumer messages. The state teams also proposed to identify subject matter experts to be used in the various education forums. Another state team reported that current events, such as those related to widely publicized breaches or other unapproved releases of personal information, will greatly influence receptivity of messages and acceptance of those messages.

Again, funding was a frequently cited barrier, as were stakeholder buy-in and political support.

Implementing Multistate Solutions

Nineteen state project teams discussed the importance of transcending state lines to provide quality and continuity of care for individuals traveling between states to receive their health care, but only a few state project teams proposed plans for multistate exchange. Four states proposed potential solutions that had specific tasks or time frames, while another 11 state teams articulated the desire to collaborate with other states on a particular issue and 5 additional state teams indicated a desire to pursue more organized plans but felt that additional time and continued networking support were needed in order to achieve a more structured collaborative environment for multistate solutions.

Few of the states proposed specific plans for the creation of a governance structure that would oversee the creation of common privacy policy and security solutions between multiple states, although a handful of states noted a willingness to join in such an effort if one were started. Three states mentioned the possibility of coordinating efforts in their own states with the efforts of a common coordinating body such as the State Alliance for e-Health. One state indicated that it planned to convene a “multistate work group” that

would track the direction in which neighboring states were going in a variety of different areas and feed that information to other state-level work groups (clinical, technical, legal/policy, etc).

State project teams noted a need to develop a plan for sharing data across state borders in the case of disaster or emergency and continuing to explore legal templates that could be shared between states. Three state project teams planned to pursue standard policies with other states concerning emergency or "break the glass" procedures. One state project team clearly outlined a plan to expand the state effort through its department of health and department of emergency management to pursue communications plans and strategies in the case of a bioterrorist attack or natural disaster into a regional plan. Three other state project teams proposed to standardize the criteria used to identify a patient within an electronic exchange. Three state project teams mentioned the need to standardize consent practices across state boundaries. However, no plan details were provided.

One state project team discussed working on a model state law to improve interstate communication and another state project team suggested working with the National Conference of Commissioners on Uniform State Laws as part of a general review on harmonizing federal and state law. Again, specific goals were not outlined in terms of formulating or utilizing model laws. Two state project teams proposed specific plans to pursue a compact between 3 states before the end of 2008 that would seek to clarify the legal interstate environments related to each state's electronic health information exchange programs. Further, the state project teams proposed to standardize laws between neighboring states that protect genetic information and define *age of consent*.

Four states proposed plans to create regional standards for technical issues, including the development of a core set of privacy and security solutions. None of the state project teams proposed multistate outreach or education plans.

Implementing National Solutions/Recommendations

The state project teams were charged with solving issues at the state level rather than making recommendations for action at the national level, unless necessary to accomplish their state-level goals. The state teams that did include recommendations for actions to be taken at the national level indicated that it would simply be more expedient to implement some standards at the national level than to try to achieve consensus within and across states.

Most of the state project teams expressed a desire to see greater coordination of governance, policy, regulation, technology standards, and education at the national level rather than in scattered regional pockets. Twenty-one states made some type of recommendation regarding national-level intervention. A number of states offered to participate in leadership and the development of policy and technical standards, especially

when they felt they had already made significant headway through local initiatives. The theme, however, clearly indicated a strong feeling that these efforts should be centrally coordinated and not left completely to local efforts, which can be scattered and lack adequate resources. There is a shared understanding that central coordination will provide for efficient knowledge transfer between state project teams that will advance the initiative nationwide.

Seven states proposed recommendations for federal guidance on practice and policy. First, although the states recognize that the variation in the way approval policies such as consent and authorization are defined and implemented is largely driven by state laws, there is widespread confusion when organizations try to reconcile the requirements of state law with federal regulations that are more stringent with regard to specially protected data. Three states suggested that a basic or core set of practices and policies for consent and authorization could be defined and coordinated at the national level so states could choose to adopt those that best met the needs of the state.

Three states suggested that federal policy guidelines regarding certain data elements would greatly reduce the burden of developing technical standards. Two states suggested using the American Society for Testing and Materials (ATSM) continuity of care record (CCR) as a policy adoption target that would encourage the development of a data set that health care providers would feel comfortable using. It is important to note here that the Health Information Technology Standards Panel (HITSP) has endorsed the work done by ATSM and Health Level 7 (HL7) to harmonize their respective standards to create the continuity of care document (CCD). The CCD describes the use of the CCR standard data set so it could function within the broader capabilities of HL7's clinical document architecture (CDA).

Twelve states proposed the need for legislation or guidance at the federal level.

Three states suggested the need for new legislation or guidance concerning HIEs or other clearinghouse organizations to enable information sharing between state-level HIEs. The federal legislation would designate a federal privacy and security standard that preempts more stringent state legislation in connection with information that is sent from one state to another via a health information network. The state teams also recommended that the legal status of HIEs be addressed at the national level, as well as the process of developing a framework for liability that addresses the role of the state-level HIEs and the interaction of federal and state-level regulatory frameworks.

Medicaid: One state team suggested that federal guidelines related to Medicaid data release be reviewed and streamlined. The desired outcome would be changes to both federal and/or state guidelines related to sharing of Medicaid data. Another state asked both the Centers for Medicare & Medicaid Services and the Office of Inspector General for a favorable advisory opinion excepting some specific level of cooperation between physicians

and hospitals with respect to sharing money for technology or participating in demonstration projects.

Stark and Antikickback Laws: Two states suggested expanding the scope of these regulations to target providers who serve the historically underserved, and to amend these regulations such that hospitals are allowed and possibly induced to provide physician practices that are serving economically disadvantaged populations with not only hardware, software, and training, but also additional technical resources to implement and support the technology.

Clarification of HIPAA Privacy Rule: Three states suggested clarification or changes to the HIPAA Privacy Rule. One recommendation was to change the HIPAA Privacy Rule so that it would require the provider to obtain a patient's legal permission once at the initial point of service that would permit the provider to release the information for specific purposes and to specified entities in the future. The suggestion to make patient permission mandatory for current exchanges for treatment, payment, and health care operations was thought to facilitate future requests for the release of the information held by that specific provider. The state team believed that making this a federal recommendation or standard would facilitate the interstate exchange of information.

42 C.F.R. pt. 2: One state suggested that HHS explore the contours of consent/approval without the need for legislative action although they also recognized that their suggestion may require congressional action. The team is recommending that HHS more clearly define 42 C.F.R. pt. 2 so that a single consent would allow for unlimited downstream releases for certain purposes and clarify that authorization can describe generally the entities to which Part 2 records may be disclosed. As an alternative, 42 C.F.R. pt. 2 could be amended to provide that patient authorization is not required to exchange the data for treatment purposes only.

CLIA: One state discussed the Clinical Laboratory Improvement Amendments, detailing specific conflicts that it imposes in their state due to ambiguity about the terms utilized. One other state proposed to review the CLIA regulations in light of HIE organizations that endeavor to provide electronic laboratory reporting services.

FERPA: Two states called for general clarification and/or revision of the Family Educational Rights and Privacy Act and educational institutions' rights to deny medical record release. It is important to note here that FERPA falls under the authority of the Department of Education.

Three state teams outlined recommendations to provide education and outreach at the national level, citing the need for a national information campaign that provides consistent and uniform messaging in the form of federally recommended education materials to include patient-consumer advocacy components and promote the idea of patient rights.

Overall the state teams are looking for a centrally coordinated effort because although the decisions need to be made at the local level, the teams do need to provide some assurance to their stakeholders that they are not operating in a vacuum and that the work they are doing will not only advance the work in their state but will also be compatible with the broader nationwide effort. It is clear that many of the teams are not fully aware of the breadth and scope of activities that are already occurring at the national level and that will serve as resources for the state teams as they move forward into implementation.