December 29, 2006

Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variation Executive Summary

Prepared for

Susan Christensen, Senior Advisor
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, Director, 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 No. 290-05-0015
RTI Project Number 0209825.000.004.002

RTI Project Number
0209825

Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variation Executive Summary

December 29, 2006

Prepared for

Susan Christensen, Senior Advisor
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, Director, Office of Policy and Research
Office of the National Coordinator
330 C Street SW
Switzer Building, Room 4090
Washington, DC 20201

Prepared by

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

List of Authors for Summary Report

Amoke Alakoye, MHS, RTI International
Chris Apgar, CSSP, CISSP, Apgar & Associates
Robert F. Bailey, BA, RTI International
William Braithwaite, MD, PhD, Braithwaite Healthcare Consulting
John Christiansen, Christiansen IT Law
Linda L. Dimitropoulos, PhD, RTI International
David H. Harris, MPH, RTI International
Mike Hubbard, Womble, Carlyle, Sandridge & Rice, PLLC
Cynthia L. Irvin, PhD, RTI International
John Loft, PhD, RTI International
Barbara L. Massoudi, MPH, PhD, RTI International
Stephanie Rizk, MS, RTI International
Walter Suarez, MD, CEO, Institute for HIT/HIPAA Education and Research

List of Reviewers

Holt Anderson, Executive Director, NCHICA
Ryan Bosch, MD, George Washington University Medical Faculty Associates
Gary Christoph, PhD, CIO, Teradata
Carolyn Hartley, Physicians EHR
John McKenney, SEC Associates
Kathleen Nolan, Director of Health Policy, Center for Best Practices, National Governors Association
Anna Orlova, Public Health Data Standards Consortium
Joy Pritts, PhD, Health Policy Institute, George Washington University
Harry Rhodes, MBA, RHIA, CHPS, AHIMA
Michelle Lim Warner, MPH, Center for Best Practices, National Governors Association

EXECUTIVE SUMMARY

This report is the first in a series to be produced under RTI International's contract with the Agency for Healthcare Research and Quality (AHRQ). The contract, entitled Privacy and Security Solutions for Interoperable Health Information Exchange, is managed by AHRQ and the Office of the National Coordinator for Health Information Technology (ONC). The following report is a summary of 34 separate interim reports submitted by 33 states and one territory as subcontractors to RTI; these subcontractors form the Health Information Security and Privacy Collaboration (HISPC). The Interim Assessment of Variation of Business Practices, Policies, and State Law (IAV) comprises the first reports submitted by the 34 subcontracted state teams and represents a "first look" at the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange (eHIE). This summary report captures the highlights from the 34 reports and presents some of the major crosscutting themes that have been raised during this first phase of the project.

This summary report consists of 3 major sections:

- Methodology
- Descriptions of Business Practices by Scenarios
- Critical Issues and Observations

The purpose of the IAV is to illustrate, in a descriptive report, the variations among the organization-level business practices, policies, and laws, as related to privacy and security, that were identified by each state team. The term *law* as used here refers to regulatory, statutory, or case law that serves as the primary driver behind a business practice. The data supporting this report come from work conducted by the Variations Work Groups (VWG) and Legal Work Groups (LWG) of each participating state team. The interim reports will be used to inform efforts of the Solutions Work Groups (SWG) and Implementation Planning Work Groups (IPWG) as the state teams continue to draft their interim reports. It is important to note that the interim reports are but a "snapshot" of a point in time in an evolving process as the state teams work with stakeholders to think through the multitude of privacy and security issues related to eHIE and as they work toward developing privacy policy and security standards to address the needs of their local communities.

Although each state team followed a core methodology, ample opportunity remained to tailor the process to meet the needs of each participating state and territory. The reports include a section that documents the process used to generate the set of organization-level business practices for each scenario, including outreach to the broader stakeholder groups, and a description of the membership and stakeholder representation of the VWGs and LWGs.

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

Table ES-1. Purposes of Health Information Exchange (HIE) and Relevant Scenarios

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

Finally, each state report provided a summary of the critical observations and key issues to bring focus to areas that the SWGs and the IPWGs should further explore.

In Section 3 we describe 10 issues that have been raised by the state teams in the interim reports and that have broad implications for nationwide eHIE. This section provides a brief overview of these topics, which is not intended to be a thorough analysis of the issues or their implications but rather a descriptive treatment of the issues. The expectation is that additional issues will be raised as the work continues and a fuller explication of the implications will be provided in the final Assessment of Variation and Analysis of Solutions reports.

HIPAA Privacy Rule Interpretations and Applications

Many business practice variations existed because of different interpretations of the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy

Rule. The most commonly mentioned was variability in the use and implementation of patient consent or authorization across organizations. Many of the reports indicate a lack of understanding on the part of the stakeholder community about the HIPAA philosophy that the privacy rules are not intended to create any barrier to the use of personal health information for treatment of the patient and that patients should expect their information to be routinely used for purposes of treatment, payment, and health care operations (TPO) unless exceptions are negotiated with the provider. Others seem to understand this approach but see conflicts with traditional practices and local laws, or at least variability in the processes of implementing practices. Section 3.1 summarizes key examples from the states regarding specific HIPAA-infused barriers to eHIE.

HIPAA Security Rule Interpretations and Applications

A review of state reports indicated some confusion and misunderstanding surrounding what appropriate security practices are, but also indicated misunderstandings regarding what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust between organizations and on the part of consumers was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule. Sometimes the matter was simply that, even though HIPAA accommodates scalability in security programs, organizations voiced concern related to liability when one organization that believes its security program is more robust sends protected health information (PHI) to another organization with a less robust security program.

There also appeared to be confusion about the different types of security required by the HIPAA Security Rule. The Security Rule addresses administrative, physical, and technical security. Even though more than one third of the rule addresses administrative security requirements, many organizations focused more attention on needed technology than on administrative safeguards.

Trust in Security

Trust was a critical issue raised in many of the state reports, as it affects the potential viability of eHIE. Specifically, 2 kinds of stakeholders expressed concerns: providers and consumers. Providers were principally concerned about liabilities possibly arising from the activities of other participants in HIE and about consumers' lawsuits for inappropriate disclosures of their information; they were concerned secondarily about potential uses of information about consumers by payers and the government. In contrast, consumer concerns tended to focus on privacy risks arising from the implementation of new technologies and the potential for unauthorized disclosures of sensitive information to payers and employers.

The leading trust issue was providers' fear of lawsuits and liabilities associated with eHIE. This issue was identified by 10 reports and was based in most cases on the fear of liability for errors or improper actions by other parties participating in HIE. One state team identified this fear as its single most significant issue, one which had been repeatedly raised and the reason providers were not willing to engage in eHIE. It is not clear whether there is much experiential basis for this fear in most states, but one identified as a concern a specific statute giving patients a cause of action for inappropriate disclosure, and another reported that HIPAA-based claims are being included in lawsuits by patients frequently enough that one provider had reported 6 such claims within the preceding 6 months. (The specific legal basis for such claims was not identified. HIPAA does not provide a cause of action for individuals.)

The second most significant trust issue was consumer lack of trust, which appeared to have been expressed directly by consumers in 4 reports and was apparently an issue perceived by nonconsumer participants in 6 others. The principal basis articulated for this lack of trust was concern about payer and employer access and, secondarily, distrust of new technologies. It appears that one major reason for this sense of mistrust is the substantial number of security breaches that have been reported over the last few years, including several involving health care organizations.

The most significant general impression that arose from this review was that trust concerns, particularly of providers, appear to be directly correlated with eHIE experience. In other words, providers in states with relatively few eHIE activities, or a briefer history of such activities, appear to fear they may be held liable or be penalized for engaging in them and, in some cases, do not trust the technologies. Providers in states with more experience in eHIE do not report the same concerns, or they report them to a lesser degree.

Finally, one noteworthy finding is that 2 state teams reported reliance on good faith and personal relationships in current practices and identified this as a positive value participants wish to preserve.

State Laws

The stakeholders identified a number of difficulties with the state laws governing privacy and security, including a general misunderstanding of the intersection between state law and HIPAA, as well as some general confusion about where state law was found and how it should be applied. In addition, when state law was readily identified and understood, it was often too antiquated to apply sensibly to eHIE.

In fact, the leading issue was the absence of state laws clearly applicable to eHIE (sometimes referred to in the reports as "laws pertaining to RHIOs" [regional health information organizations]), which was identified by 11 state teams. Ten state teams identified the generally confusing conditions of state laws as a critical issue, and,

consistently, 11 state teams reported the use of overly conservative business practices due in large part to confusion or lack of knowledge about state laws. ("Overly conservative" in this context means more restrictive in terms of information sharing than is actually required by law.)

At least 2 states noted that a number of stakeholders, particularly providers, were unaware of the need to comply with state laws that are more restrictive than HIPAA and were, in effect, treating HIPAA as a ceiling rather than a floor. One caveat in reviewing these reports for awareness of state law is that state teams were asked to identify only state laws that provided the underlying rationale for a specific business practice; they did not engage in a comprehensive legal analysis of their entire body of state law governing privacy and security. Confusion about sharing information for law enforcement, public health, and bioterrorism purposes, in particular, appears to be a critical problem, given concerns about possible bioterrorist incidents, natural disasters, pandemic flu, and other mass crises. Current practices appear to rely heavily on good will, which is necessary but perhaps not sufficient, especially when interstate coordination is necessary.

Intersection With Other Federal Laws and Regulations

The state reports included a number of examples of challenges involving the intersection of state laws with HIPAA and other federal laws and regulations.

In the early 1970s, Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, so it enacted legislation that gave patients a right to confidentiality. For the almost 3 decades since the federal confidentiality regulations (42 C.F.R. pt. 2) were issued, confidentiality has been a cornerstone practice for substance abuse treatment programs across the country. These regulations protect all information about any person who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program. The 42 C.F.R. pt. 2 regulations generally require patient consent (authorization) prior to disclosure of information, except in emergency situations.[1] These restrictive requirements pose a challenge to the exchange of health information.

There are differences in providers' treatment of patient medical information when substance use is involved: variation exists in the treatment facilities', physicians', and integrated delivery systems' understanding of 42 C.F.R. pt. 2, understanding of the relation of 42 C.F.R. pt. 2 to HIPAA, and the application of each. Treatment facilities note stringent precautionary measures to safeguard patient substance use information: while physicians comment on limited or restricted access to patient medical files, treatment facilities note that patient files are kept in a locked cabinet behind a double-locked door.

[1] *Consent* is the term used in 42 C.F.R. § 2.31, "Form of written consent."

The state reports show that, although the stakeholders representing treatment facilities in participating states demonstrate a general understanding of 42 C.F.R. pt. 2, other health care providers are less familiar with the regulation's requirements. The complicating factor is that the differences between HIPAA provisions and 42 C.F.R. pt. 2 provisions create ambiguity about which regulation applies and under what conditions. Consequently, variation in both policy and practice increases across an array of stakeholders. The differences in language and drivers for each regulation create further ambiguity, leading to increased variation in how the regulations are applied by stakeholder organizations. The result in current practice is that, without a provider's clear understanding of the requirements for both HIPAA and 42 C.F.R. pt. 2, protected information might be shared because that provider understands that HIPAA allows sharing of health information for treatment, even though sharing without patient authorization would be prohibited under 42 C.F.R. pt. 2.

One state team referred to Clinical Laboratory Improvement Amendments (CLIA) as a barrier to eHIE. CLIA defers to state law for the purpose of determining the permissible recipients of laboratory results. Many state laws very narrowly define those persons who are authorized to receive test results, and variation among state laws has created a medley of different standards.

Under CLIA regulations, 42 C.F.R. § 1291(f) states, "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." The term *authorized person* is defined in 42 C.F.R. § 493.2 as "an individual authorized under state law to order tests or receive test results, or both." The term *individual responsible for using the test results* is not defined in the CLIA regulations, and there is significant uncertainty as to its meaning.

One state team also raised as a potential barrier to electronic prescription data exchange the federal regulation 21 C.F.R. § 1306.11, which requires that the original, written, signed prescription be presented to the pharmacist for review before the dispensing of a controlled substance. Another state team mentioned the Employee Retirement Income Security Act of 1974 and wrote that "the limit and boundaries of the Employee Retirement Income Security Act, 1974 are not clear" in relation to state law; there was also a mention of the Family Educational Rights and Privacy Act.

Networking Issues

Most state teams reported quite limited interorganizational exchanges of clinical information being done electronically for 3 reasons: (1) absence of regional eHIE networks, (2) limited deployment of electronic health record (EHR) systems, and (3) lack of interoperability in those EHR systems that have been deployed. eHIE between organizations is limited mainly to content-specific clinical messaging in the areas of pharmacy/prescription drug information (e-prescribing), laboratory data, and radiology/digital imaging data. Across

many states a significant number of pilot projects are under way to test various eHIEs, including emergency department data and public health data.

Significant capacity gaps and variations exist in the level of resources, technical capabilities, and financial means of organizations (ie, large versus small, urban versus rural). These gaps create significant variation in HIE practices among organizations; in turn, these variations in HIE practices limit or restrict the ability of organizations to conduct interorganizational HIEs (lack of compatible systems, lack of compatible practices, lack of trust). State teams also noted that different types of HIE (ie, provider-to-provider, provider-to-payer, payer-to-payer, and between others) require different handling.

Individual states are at very different stages in the development of networks that facilitate the interorganizational exchange of clinical health information electronically. Some states altogether lack initiatives to establish such network infrastructures; some are beginning to organize their communities, but no infrastructure approach has been identified, selected, or adopted; some have implemented limited-scope efforts to connect a small number of organizations within a region in the state (subregional networks); and only a very few have a state network infrastructure. A common concern across state teams was the lack of well-defined, operational, and deployable models for regional networking.

There are many definitions of what RHIOs are and many definitions of their roles, functions, funding structure, and so on. There were significant concerns among the state teams about the legal status of such organizations, their ability to legally operate such eHIEs, their ability to store and maintain data, and the like. This lack of experience with organizations designed to govern electronic data exchange, as well as the uncertainty about their legal status, carries implications for stakeholders seeking to design and put into practice consensus-based privacy and security solutions: such organizations could serve as the mechanism by which many decisions are implemented and enforced.

Linking Data From Multiple Sources to an Individual

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to eHIE. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use or disclosure of PHI on the wrong patient, which is both a clinical and a privacy risk. This risk is particularly acute when information is shared across institutions that differ in their methods of patient and record identification.

Patient and provider identification across organizations is required in order to

- improve administrative efficiencies and reduce health care costs by minimizing the collection of redundant information and by reducing or eliminating the need to perform redundant tests (because of the inability to access information about a patient in a timely fashion);

- provide better-quality care, avoid medical errors, and improve patient safety;
- control against identity theft, fraud, and abuse;
- appropriately match data about an individual from one organization to another when HIEs are performed;
- appropriately authenticate a patient or a provider to come into an organization's system;
- establish access controls to certain health information on the basis of the authenticated identity of a patient or a provider;
- implement mechanisms to prevent inappropriate access to data or monitor the access to data by patients and providers; and
- implement core eHIE functionality.

Recent developments in the area of personal health records have also advanced the need to establish a consistent, reliable method for linking patients to their records so that authorized providers and other users can locate the right information about the right patient.

The variability in methods across organizations to match patients to their records and the lack of agreed-upon patient-to-record matching standards to apply during interorganizational HIEs were perceived as major challenges by many state teams. This was not the case for uniquely identifying *providers* across the health care system, because new federal HIPAA regulations have now established a national, standard unique identifier for health care providers (the National Provider Identifier, or NPI).

Current practices reported by participating stakeholders from most state teams pointed at organizations' use of unique, asynchronous, and incompatible methods to establish the identity of their patients, enrollees, clients, and consumers. State teams reported instances in which even within an organization the same patient had been assigned more than one ID within that organization (eg, a patient's ambulatory or primary care clinic record vis-à-vis the same patient's inpatient or hospital record). Although multiple IDs for the same patient are often caused by errors such as spelling variations in names and transpositions of dates, some hospitals intentionally assign a different identification number to the same patient for each admission. Most state teams also emphasized the need to establish standard mechanisms to identify patients across organizations as a foundational component of the evolving eHIEs.

State teams specified challenges associated with the variability and incompatibility of patient identification systems and approaches, including

- inability to appropriately link patient information across systems for delivery purposes (applicable to both paper and electronic environments);
- inability to create longitudinal, multifacility continuum-of-care episodes for a patient;

- inability to track patients across a full episode of care and monitor performance of health care systems (public health functions); and
- lack of interoperability across systems for purposes of identifying providers, which forces a patient's providers to "jump" from one system to the next to gather and manually integrate all information available on him or her instead of using automated methods to aggregate the information across sources.

The state teams were acutely aware of the potential risk increase for privacy violations and identity theft when a unique patient ID is implemented across institutions or regions. State teams also cited the need to counter possible negative public reaction with effective security controls and extensive consumer education.

Interstate Issues

Although the identification of interstate issues was not a primary focus of the interim assessment of variation, 16 state teams reported that interstate issues should be considered carefully, though it is not clear that the issues cited posed critical barriers to eHIE. Typically, states raised interstate issues for one of two reasons: (1) either there is considerable sharing of health care facilities across state lines, or (2) whenever the state experiences very large seasonal inflows of both out-of-state workers and tourists its residents make substantial use of out-of-state providers and a number of interstate health systems and plans have facilities and do business in the state.

One markedly rural state noted that, because of its relative scarcity of certain kinds of health care facilities, access to other states' hospitals and specialty services is crucial for its residents; in fact, for this state any meaningful health information infrastructure would have to reach major metropolitan areas in 3 other states. The legal variations noted as potential barriers to eHIE include differences in standards for genetic information; electronic prescriptions; immunization, HIV/AIDS, and minors' rights; minors' consents; and workers' compensation, mental health, and substance abuse.

In addition to reporting interstate issues, at least one state team reported that agreement to reduce variations between state and American Indian tribal standards is critical to developing statewide eHIEs. Several state teams noted that they did not believe that interstate issues were problematic and indicated that the disclosing state's law generally controlled. Most issues were between organizations rather than between states, and interstate issues tended to be resolved within organizations.

Disclosure of PHI

Overall, state teams consistently identified the business practice variations related to the disclosure of health information as the single most significant set of factors affecting the ability to conduct eHIE between organizations. Disclosure-related factors affecting eHIE, as identified by states in their interim reports, are

- general lack of consistent and accurate understanding of federal and state laws and regulations with respect to disclosures, as well as the corresponding effect on the variability of business practices;
- issues surrounding the interpretation, requirement, and use of patient consent or patient authorization in connection with the release of health information;
- issues related to the re-release or redisclosure of health information received by one entity from another;
- issues related to the HIPAA *minimum necessary* requirement;
- issues of ownership and control of health information;
- differences in the way certain health information must be treated and handled because of local, state, and federal regulations that consider that kind of information to have a higher degree of sensitivity;
- the need to ensure that under medical or health emergency circumstances health information is able to be exchanged fast, easily, and securely;
- varying degrees of reporting requirements for public health purposes;
- handling of disclosures related to judicial proceedings and law enforcement;
- burden imposed by the need to document certain disclosures of health information; and
- other issues, including importance of human judgment factor in determining disclosure, and the validity, applicability and acceptability (legal and otherwise) of digital signatures to support patient consent and patient authorization procedures.

Cultural and Business Issues

State teams referenced a number of cultural and business issues that pose challenges to eHIE. One example is concern about liability for incidental or inappropriate disclosures, which causes many stakeholder organizations to take a conservative approach to developing practice and policy. At least one state's patient consent requirements place all responsibility and liability for the appropriate release of patients' health information on the health care provider *releasing* information and place no responsibility on health care providers *requesting* the information.

Another example of a business issue that poses a challenge is general resistance to change, which is a common issue that organizations face whenever there is a change in how business is conducted. This is frequently cited as a cultural issue in discussions about decisions to adopt electronic systems. There is a certain comfort with existing paper-based or manual systems and data exchange practices and processes, and there is a general belief that current manual practices are timely, effective, and productive of accurate data. Implicit in some of the discussions is an assumption that security slows down the process, in the sense that the data are secure but are not transmitted as fast as they can be with a quick phone call.

In fact, most exchanges occur person to person, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be crucial to include these points at which human judgment is required in the specifications for any system developed to exchange information.

Technology adoption gaps (large versus small, urban versus rural), costs of systems, processes to address security domains, and lack of resources must also be addressed.

A third business issue that cuts across all the scenarios and domains is the need for clear definitions of terms within state and federal laws. For example, terms like *medical emergency, current treatment, related entity,* and *minimum necessary* do not have agreed-upon definitions and therefore serve to increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization. For example, there is the term *health record*. Disagreement exists about whether or not a patient's demographic data and a pointer to the location of a patient's health information constitute a *health record*.

Another cultural issue that was raised involves the tension between health care providers, hospitals, and patients concerning who controls or owns the data. A number of providers indicated that they did not think that patients should have full access to their records, especially to doctors' notes. A concern was that doctors would not enter complete notes if the patient would be able to access the record. Concerns about liability also emerged. Despite these concerns, the majority of stakeholders agreed that eHIE should be designed in ways to address patients' needs, interests, and concerns and that doing so is critical to the success of eHIEs.