BNA's

HEALTH CARE POLICY

REPORT

VOL. 15, NO. 42

OCTOBER 29, 2007

Health IT: Is It Safe to Exchange Data Yet?

BY SUSAN M. CHRISTENSEN

It is tempting to believe that the United States has made little progress in the critical area of protecting the privacy and security of electronic health information. But important work has been done and is now available to inform a policy discussion about privacy and security issues in health care. This paper will provide a brief overview of a major nationwide initiative with examples of findings and recommendations.

In the last year, 33 states[1] and Puerto Rico have proposed solutions and implementation plans to address the confusing and conflicting privacy and security requirements they identified. Another initiative will build upon these state efforts, as described below. All of this is designed to provide the guidance and resources needed to build and run secure and trusted health data exchanges.

One important lesson from the process: Privacy and security issues must be addressed whether or not health information is exchanged electronically or on paper. The work revealed significant problems in *current paper-based* environments, and moving to electronic data exchange—combined with the significant trust-building work that is required to do so—can mitigate many of those problems.

Although privacy *policy* (when should consent be required?) and security *standards* (how do we protect data?) are intertwined, they are two different things. A decision about privacy policy is best made by a data exchange community so that it reflects local or regional interests, while robust security standards must be adopted nationally and even internationally, so that there is an assurance of security against breaches and the ability to enforce privacy decisions even when data are sent to a distant user.

Susan M. Christensen is a senior public policy adviser at Baker, Donelson, Bearman, Caldwell & Berkowitz PC. From 2000 to 2004, she served as former Congresswoman Nancy Johnson's (R-Conn.) senior health policy counsel. Prior to joining Baker Donelson, Christensen most recently served as senior adviser for the Agency for Healthcare Research and Quality in the U.S. Department of Health and Human Services. While at AHRQ, she was responsible for managing key policy issues related to the agency's overall health IT portfolio, including the work with contractor RTI and six state-level health information exchange initiatives. This paper does not represent the views of AHRQ or HHS.

[1] Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Mississippi, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Puerto Rico, Rhode Island, Utah, Vermont, Washington, West Virginia, Wisconsin. and Wyoming.

Privacy and Security Solutions for Interoperable Health Information Exchange

In 2005, the Agency for Healthcare Research and Quality (AHRQ)[2] contracted with RTI International to engage in an $11.5 million, 18-month nationwide analysis of privacy and security issues that arise in deploying health IT and establishing electronic health data exchanges.

Key Features

The work conducted so far on health data information exchange includes:

- More than $20 million invested by the Department of Health and Human Services;
- More than two years of effort nationwide by the contractors, states, and communities, including over 1,600 health care stakeholders and public officials;
- Thirty-three states and Puerto Rico, each under the auspices of its governor's office, and working within their jurisdictions as well as collaborating regionally and nationally, identified issues, proposed solutions, and developed implementation plans to assure the privacy and security of health information in their jurisdictions and across jurisdictions;
- Issues of regional and nationwide significance were identified by the state teams and submitted with recommendations to HHS and the State Alliance for eHealth.

More information can be found at *http://healthit.ahrq.gov*.

Under its contract, and working with the National Governors Association (NGA), RTI subcontracted with 33 states and Puerto Rico to (1) document variations in organization-level privacy and security business practices, policies, and state laws that affect electronic health information exchange; and (2) identify and propose practical ways to reduce the variation to those ''good'' practices that will permit interoperability while preserving the necessary privacy and security requirements set by the local community. The collection of state teams has come to be known as the Health Information Security and Privacy Collaboration, or HISPC.

Along with the contracted staff, over 1,600 stakeholders across the country participated in organized working groups, using 18 common scenarios for their discussions and generating their analyses of the privacy and security landscape in their state. RTI and NGA also conducted individual site visits, regional meetings, and a national meeting (with a second national meeting under the RTI privacy contract upcoming Nov. 1-2 in Washington, D.C.; see http://www.rti.org/hispc), to encourage knowledge sharing and solution development by the state teams. A number of reports summarizing the work and making recommendations have been released. They can be found at healthit.ahrq.gov/privacyandsecurity. A good sense of the overall project can be found in the *National Summary* and the report on final implementation plans.

Over the course of the contract, additional funding has been provided—bringing the total to approximately $20 million—and the scope of work expanded to meet the needs of the state teams. In addition, all U.S. states and territories have been invited to participate in the working groups and meetings, broadening the impact of the overall project.[3]

Other observations from the process:

- Trust involves more than compliance with privacy and security laws and regulations. Regardless of where the legal bar is set, because of differing community standards, each exchange community tends to interpret legal requirements somewhat differently as well as impose other unique restrictions on data exchange.
- While guidance on federal laws and regulations is clearly needed, the state teams almost uniformly felt that most of these issues must be identified and addressed at the state and community levels. States did recognize that they also must understand and come to agreement about these issues with neighboring jurisdictions as their data exchanges expand.
- The process of resolving these issues is just as important as the final policy decisions that are reached. The process itself builds the trust needed for health information exchanges to be secure and successful; privacy and some security policies imposed from outside sources may be less likely to be adopted because they do not flow from these hard-won trusted relationships.
- Consumer involvement is difficult to secure, but the state teams recognized such involvement is essential in order to reflect consumer interests adequately and serve as a check on cultural competence.

Proposed state-level solutions fall into five categories:

- Practice and Policy—including agreed-upon interpretations of the HIPAA privacy rule and developing uniform consent approaches.
- Legal and Regulatory—with regard to both state laws (finding and interpreting; application to electronic health data exchange) and their intersection with federal law.
- Technology and Standards—data security (four As: authentication, authorization, access, and audit); transmission; patient identity management; and segmenting data (particularly sensitive data).
- Education and Outreach—for providers, consumers and policymakers.
- Governance Models for Solutions.

Recommendations for national action—some examples from the reports:

While the state teams were charged with solving issues at the state level, they did include recommendations for actions to be taken at the national level that they indicated would simply be more expedient rather than try to come to consensus within and across states. Most teams wanted greater coordination of governance, policy, regulation, technology standards, and education at the national level rather than scattered in regional pockets. Below are some excerpts, to illustrate the level

[2] The contract is co-managed with the Office of the National Coordinator for Health IT (ONC) in the Department of Health and Human Services (HHS).

[3] In addition, follow-on contracts are currently being planned by ONC.

of detail reached. Note that this is just a small sampling of the recommendations.

Seven states proposed recommendations for federal guidance on practice and policy. Although the state teams recognize that the variation in the way consent and authorization policies 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, especially with regard to specially protected data. Although most of the state teams developed plans to create uniform approval policies within their state, three state teams suggested the variation in approval practices could be resolved more expediently if a basic or core set of practices and policies for consent and authorization could be defined and coordinated at the national level so that states could choose to adopt those that best met their needs.

Although many states proposed legal and regulatory solutions at the state level, twelve states indicated that they would like to see legal and regulatory guidance at the national level. These suggestions took on two major themes: (1) passing new federal legislation/regulatory guidance concerning health information exchanges or other clearinghouse organizations in order to enable multi-state data sharing, and (2) providing clarification/updates to current legislation.

Six states outlined suggestions for standardizing data technology and data standards at the national level. Many of these states expressed the feeling that there needed to be clearer examination of the role of an emerging standard-setting organization as a mechanism to respond to an evolving interoperable environment more quickly and effectively than state-by-state or federal legislative processes.

A number of other states echoed the need for national standards with regard to the following:

- Standards need to be developed for role-based access control as defined initially by the Health Insurance Portability and Accountability Act (HIPAA) rules with regard to treatment, payment, and health care operations, and covered entities, and then expanded to non-covered entities and individuals or entities likely to have access to data.

- The electronic health record audit trail, documenting by time and date stamp and source for all read and write access to protected health information, currently required under the HIPAA security rule, should be reinforced and required under state regulations for all electronic health information exchange.

- Consumers should have the option to receive automatic reports each time their records are accessed. In addition, there should be a standard process for consumer-initiated data review and correction to ensure the integrity of data.

- A model for appropriate security standards practices should be formulated that includes a review of all existing security standards and a data classification schema.

For the complete set of recommendations, see the reports at http://healthit.ahrq.gov/privacyandsecurity or http://www.rti.org/HISPC. Some of the state teams posted their findings and recommendations, and they can be reached through the RTI site.

A lot of the work accomplished under the RTI contract will be utilized in other efforts, including the State Alliance for eHealth work.

State Alliance for eHealth

The State Alliance for eHealth is a collaborative body, managed by the NGA under a contract with ONC, that provides a nationwide forum through which stakeholders can work together on inter- and intrastate-based health information technology policies and best practices. (See http://www.nga.org/center/ehealth.) According to its Web site, it is a consensus-based, executive-level body of state elected (and appointed) officials convened to address state-level health IT issues.

The State Alliance for eHealth has been organized to:

- From a state-specific perspective, address barriers to health information exchange and adoption of health IT, while preserving privacy, security, and consumer protections.

- Build consensus in seeking the harmonization of the variations in state policies, regulations, and laws, where appropriate, and develop standards and/or guidance for modifying such policies, regulations, or laws.

- Allow for dialog among states that will fuel creativity and partnerships among states and with the private sector in the health IT arena.

- Allow for the appropriate input of experts and others working on health IT endeavors to inform state policymaking.

The State Alliance has a non-voting advisory committee and, for the first year, three taskforces. Each taskforce will be composed of key stakeholders at the state level who can provide expertise and experience in addressing state-level health IT issues and present recommendations to the State Alliance. The taskforces include the Health Information Protection Taskforce, the Health Care Practice Taskforce, and the Health Information Communication and Data Exchange Taskforce.

The reports and findings from the RTI privacy and security contract described above are being considered by the State Alliance through its Health Information Protection Task force. There will be ongoing coordination to maximize the impact of both efforts.

In August 2007, the Health Information Protection Taskforce submitted its progress report to the Alliance, in which it makes findings and recommendations and sets out next steps. See http://www.nga.org/Files/pdf/0708EHEALTHREPORT.PDF. The report includes recommendations for how state and federal policymakers can work together to resolve privacy and security issues, starting on page 18. They are too complex to set out here.

Conclusion

No one working on issues related to the protection of health data can deny the complexity and seeming intransigence of the problems presented. The projects just described have not fully resolved these issues, yet they have made significant strides in documenting the landscape that surrounds us. And a process has been established that allows progress to be made by those communities ready to move forward.

More importantly, policymakers and the health care industry can now engage in a much more informed discussion than we have ever had in this area—if they take advantage of the excellent work that has been done and that is ongoing.