Establishing Mutual Trust is a Necessary Prerequisite to Achieve Widespread Exchange of Health Information

{This article originally appeared in substantially the same form in the March 2009 issue of the International Association of Privacy Professionals Privacy Advisor *newsletter.}*

The Health Information Technology for Economic and Clinical Health (HITECH) Act expands the privacy and security provisions in HIPAA to a broader set of health information exchange participants.

One of the primary obstacles to widespread adoption of electronic health records is agreeing on appropriate privacy protections for the personal information contained in medical records. Much of the current debate centers on what classes of data must be protected, how they should be protected, and under whose control. Special challenges exist where different stewards and users of health records (*e.g.*, federal government agencies, health care providers, state public health agencies, private companies) are subject to different privacy and security rules and regulations. Organizations with relatively stringent privacy requirements are understandably reluctant to share data with others subject to less rigorous requirements. Generally speaking, government agencies are subject to more stringent privacy laws and constraints on the collection, use, and disclosure of personal health information than their counterparts in the private sector, although such significant variations exist in state-level regulations that some commercial entities may also face very tight restrictions. The key point is that there is no well-defined baseline of privacy requirements for all health information exchange participants, and significant efforts will be required to arrive at a level of trust acceptable to health data owners in order for them to agree to disclose information even to properly authorized requesting entities.

Interoperability Depends on Trust

The fundamental challenge is how to establish a framework of trust among all the entities participating in health information exchange, so that the existing technical means of information sharing will actually be adopted and put into practice. This challenge was made even more pressing by the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act within the American Recovery and Reinvestment Act of 2009 signed into law on February 17. This legislation includes measures intended to strengthen federal privacy and security laws protecting individually identifiable health information from unauthorized disclosure and misuse. One implication is to expand the coverage of the requirements of the Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA) to hold all "business associates" of covered entities to the same requirements as the "covered entities" defined in the original HIPAA legislation (*i.e.*, health plans, health care providers, and health care clearinghouses). There is additional language in the law to consider certain non-covered entities as business associates, and therefore to extend privacy and security requirements to health information exchange participants such as Regional Health Information Organizations (RHIOs), electronic prescribing gateways, and other technical service vendors that provide data transmission to covered entities.

These steps go a long way toward leveling the privacy playing field in terms of information use and disclosure and in requiring explicit consent from individuals before using their health information for any purpose outside a clearly defined set of permitted uses. However, there are still significant potential players in health information exchange that remain non-covered entities, most notably including vendors of personal health records like Google Health and Microsoft Health Vault. These are data aggregation applications that depend on pulling personal health information from records maintained by insurance plans, health providers,

The law now requires virtually all public and private sector holders of protected health information to provide notification to individuals and government authorities if their health information is disclosed in a data breach.

labs, and other covered entities, so resolving the disparity in required privacy and security protections is necessary to establish sufficient trust to allow personal health record systems to function as intended. Personal health records are often promoted as the best mechanism for allowing individuals to control their own health information, including providing or revoking consent to disclose their information for specific purposes. To make this vision feasible, it is essential that personal health record systems are able to retrieve individually identifiable health information from a broad range of covered and non-covered entities. Since not all of these health information exchange participants are bound by the same rules, additional measures are needed.

Privacy Drivers Differ by Sector

As privacy practitioners are well aware, HIPAA is not the only legislative source of privacy protections for health information, so even if HIPAA coverage were broadened to apply to a wider range of health information exchange participants, there are other differences to be addressed, especially when comparing federal government agencies to commercial sector entities. U.S. federal agencies are subject to a variety of general and health-specific privacy and security regulations, most of which have no corresponding equivalent in the commercial sector. Many of these regulations have similarly worded privacy protections but differ in scope or applicability to certain types of data:

- The E-Government Act of 2002 (includes the Federal Information Security Management Act as Title III, and also requires privacy impact assessments be performed before creating new data collections containing personally identifiable information and posting privacy policies on agency websites)
- The Privacy Act of 1974 (established requirements for collection, use, and disclosure of personally identifiable information by U.S. federal agencies; applies only to U.S. citizens and permanent resident aliens)
- Title 38 of the United States Code (applies only to U.S. veterans; specific sections address privacy of veterans' claims and confidentiality of veterans' medical records)
- Title 42 of the United States Code (specifies privacy protections for data in medical records related to particular types of treatment, such as mental health and substance abuse).

Another significant point of disagreement between government and non-government entities is data disclosure, both authorized and unauthorized. All federal agencies are required to report actual and potential breaches of personally identifiable information to the U.S. Computer Emergency Response Team (US-CERT) within one hour of discovery. While the majority of states have personal data breach disclosure laws on the books, the HITECH Act established a federal data breach disclosure requirement for health information unless it is encrypted or otherwise rendered unusable. This requirement applies to vendors of personal health records as well as all covered entities and business associates, but the timeline for notification is as long as 60 days from when the breach occurs. When authorized data disclosures occur, federal agencies are further required to verify that sensitive data extracted for information systems are erased within 90 days unless its use is still required. This requirement minimizes the long-term storage of personally identifiable information by authorized requesters, and also means that for each new use of data stored in a government database, a new request must be submitted. Private-sector entities receiving this type of data from the government are not bound by these requirements, increasing the threat of secondary data disclosure and in some cases greatly reducing the willingness of federal agencies to share this data at all.

Current efforts to establish mutual trust are frustrated by the lack of technical means of monitoring and enforcing compliance. Achieving and maintaining trust remains a process of negotiation of legal agreements and manual auditing for compliance.

How then to establish the basis of mutual trust needed to enable health information exchange, and what requirements should be included? There are three general approaches to this problem: individually negotiated data sharing agreements between each pair of information exchange partners (sender and receiver); a single master trust agreement to which all participants become a party; or a combination of these two, with a master agreement setting the minimum level of trust and purpose-specific extensions or augmentations of the master agreement where needed. To reduce administrative complexity, a multi-party master trust agreement can be an attractive option – the Data Use and Reciprocal Sharing Agreement being negotiated for the Nationwide Health Information Exchange (NHIN) is one example of a master trust agreement. Unless and until some greater harmonization of privacy policies and requirements is reached between public and private sector, HIPAA covered and non-covered, state and federal, and even health and non-health data, it is likely that specialized trust agreements will continue to be used between pairs of health information exchanging organizations.

No Technical Means of Enforcement

Complicating this issue is the fact that the primary means of enforcement for privacy requirements is manual auditing for compliance in accordance with legal constructs or contractual agreements. The lack of automated technical means of enforcing or monitoring compliance with privacy rules means that enforcement of any new health IT privacy standards must rely on non-technical means. Driven in part by past experience with HIPAA enforcement the HITECH Act both increases the tiered civil and criminal penalties for violations of the privacy rules, and now requires the imposition of penalties and a formal investigation in cases of willful neglect, and also confers on state attorneys general the right to bring civil action on behalf of residents adversely affected by violations of the law.

The biggest obstacle to more effective enforcement of privacy regulations is the lack of automated monitoring and auditing methods to augment voluntary compliance and manual auditing efforts. An alternative technical approach could include tagging data with privacy requirement information and using policy evaluation and enforcement tools to validate that the provision and use of that data complies with the requirements. This idea is analogous to digital rights management measures used to limit copying and redistribution of audio and video files. One key distinction is that digital media frequently use proprietary file formats, while most information exchange and interoperability formats promoted for health information exchange rely on open data standards and protocols. The Web Services Security standards developed through the Organization for the Advancement of Structured Information Standards (OASIS) include some work on electronic representation of privacy policies (WS-Policy and WS-Privacy), but attaching the corresponding privacy requirements to data to provide the technical means of privacy compliance and enforcement remains an undeveloped opportunity. In the current environment, establishing trust among health information exchange participants remains a process of negotiation, contractual agreements, and manual legal enforcement.

Stephen Gantz, CISSP-ISSAP, CEH, CGEIT, CIPP/G, is founder and Principal Architect of SecurityArchitecture.com. He can be reached through the "Contact Us" link on the SecurityArchitecture.com website or by email at sgantz@securityarchitecture.com.

