Ensuring Privacy and Security in Nationwide Data Exchange

Save to myBoK

by Deresa Claybrook, MS, RHIT

The story made national headlines: a VA employee who worked from home had his house broken into, and a burglar stole a laptop with valuable identifying information on it. The story got a lot of publicity because of the privacy and security concerns that we all have about our personal information.

The good news is that the laptop was recovered, and the Veteran's Administration does not believe that the information was accessed. The FBI performed forensic tests on the laptop and is confident that the sensitive data were not accessed.

For those of us working to transition to portable electronic health records, this incident makes us think about the privacy and security policies that govern data exchange between organizations and states. Many HIM professionals code, transcribe, and perform other HIM functions from home offices, which could lead to a similar adverse event if we do not take protective measures and address data privacy and security. The same story could easily be one with medical information lost instead of personal information.

The HISPC Experiment

Workflow and how we process information are changing rapidly because of how we use computers and information. The Agency for Healthcare Research and Quality and the Office of the National Coordinator for Health Information Technology (ONC) have funded a nationwide effort to review business practices, policies, and state laws governing the exchange of medical data. The initiative is called the Health Information Security and Privacy Collaboration (HISPC).

The contract was awarded to RTI International and is supported by the National Governors Association. Thirty-three states and Puerto Rico were awarded subcontracts to begin this work.

The objective is to identify variations in organization-level business privacy and security practices that pose barriers to interoperable electronic health information exchange as well as good practices that enable exchange. An analysis of the policy or legal barriers will permit decisions about how to best protect privacy and security and achieve broad health information exchange. Additional goals include:

- Preserve and enhance essential privacy and security protection
- Incorporate good practices into proposed solutions
- Work toward consensus-based solutions to barriers
- Develop plans to implement the solutions

Each state has been provided with funding, training, Web site work space, and some scenarios to generate discussion, formulated by AHIMA. Each state is empowered to develop a plan of action.

Privacy Initiatives Everywhere

There are a number of other privacy and security initiatives under way, including:

- American Health Information Community (www.hhs.gov/healthit/community/background)
- ONC's Evaluation of Standards Harmonization Process for Health Information Technology (www.hhs.gov/healthit/shp.html)

- ONC's Evaluation of a Compliance Certification Process for Health Information Technology (www.hhs.gov/healthit/ccp.html)
- Nationwide Health Information Network Prototypes
- RTI International's Antifraud Requirements for Electronic Health Records (http://ehrantifrauddev.rti.org/)
- ONC's Health Information Technology Initiative (http://hitadoption.org/index.php?p=about)
- Proposed changes to anti-kickback rules

Oklahoma's Plan

Oklahoma formed a stakeholder community, and the governor appointed a steering committee. Oklahoma's steering committee selected work groups to pursue four aspects of the privacy and security study.

The state variation working group is tasked with assessing variations in organization-level business policies and practices and categorizing them as barriers or neutral with respect to interoperability. The state legal working group is assessing applicable privacy and security policies, underlying regulations, and case law. Its goal is to identify legal sources of barriers to interoperable health information exchange.

The state solutions working group is tasked with reviewing the assessment of variations of state laws and business practices identified as barriers by the state variation working group and formulate preliminary solutions to the barriers. With support from the Oklahoma HISPC team, the working group will draft the preliminary analysis of solutions report.

The last phase is the work of the state implementation working group, which will review the interim analysis of solutions and propose a preliminary implementation plan.

As part of the HISPC subcontract, a regional meeting was held in Kansas City, where neighboring states came together to discuss how they were working on the plan. Each state discussed barriers and possible strategies to meet the challenges that lie ahead in making this process happen.

If you are an HIM professional transitioning to the electronic health record or you are concerned about the privacy and security issues that surround the new technology, there are ways that you can get involved. David Brailer, former head of ONC, has stated, "Health IT can enable transformation of healthcare by allowing a better way to care-consumer by consumer, physician by physician, disease by disease, and region by region." The key is to get involved at your level and make it happen.

As HIM professionals, we have a solid knowledge of health information and we have a voice. We truly understand workflow processes. We understand the importance of privacy and security with health information and personal information. This is the area where we can make a difference. Start out by volunteering and ask to be involved with one of these state work groups.

Deresa Claybrook *(dclaybrook@cox.net) is founder of the consulting firm Positive Resource in Oklahoma City, Oklahoma.*

Article citation:
Claybrook, Deresa. "Ensuring Privacy and Security in Nationwide Data Exchange" *Journal of AHIMA* 78, no.4 (April 2007): 68-69.