Privacy and Security in an Electronic Age: E-HIM Environment Poses New Challenges for HIPAA

by Dan Rode, MBA, FHFMA

This month marks the third anniversary of the HIPAA privacy regulation. It also marks the one-year anniversary for the security regulations. HIPAA privacy and security regulations appear to be in place and working throughout the healthcare industry. However, it is clear from talk in Washington that we are in for more debate on privacy and security as the industry moves to electronic health records (EHRs) and health information exchange, be it local, regional, or national.

Recent events such as Hurricane Katrina have highlighted the need for patient authentication and the need to address the relationship between national and state standards. Nonprovider health plans and employers are also beginning to build patient portals for subscribers and employees with data taken from claims history or similar sources. These uses of healthcare data raise new concerns that were not contemplated when HIPAA was written.

Federal Initiatives to Address HIPAA

Outside of the Office for Civil Rights, the federal group that has most followed the course of the HIPAA privacy rule has been the privacy and confidentiality subcommittee of the National Committee on Vital and Health Statistics. The subcommittee has addressed the positive and negative aspects of the HIPAA regulations over the years, before and after their adoption. The group has called to the nation's attention HIPAA's effect on healthcare at educational institutions and in legal issues. Over the last year the subcommittee has worked on issues raised by a nationwide health information network (NHIN). It will present its recommendations to the secretary of the Department of Health and Human Services (HHS) in late June.

Privacy and security are also the focus of one of the first contracts awarded by the Office of the National Coordinator for Health Information Technology this past fall. RTI International of North Carolina was awarded a contract to look at the manner in which hospitals, physicians, and other healthcare organizations implement required security and privacy policies and how policies vary to meet organization needs. The variations in these policies and practices, along with those created by differing state laws, provide significant challenges for widespread EHR adoption and information exchange.

RTI will establish the Health Information Security and Privacy Collaboration (HISPC) in conjunction with a multidisciplinary team of experts and the National Governors Association. HISPC will address "variations in organization-level business policies and state laws that affect privacy and security practices which may pose challenges to interoperable health information exchange."[1] AHIMA has taken a significant role in this privacy and security project. What makes the HISPC approach different is that there will also be activity at the state level, where we expect to see the involvement of our HIM state associations and members.

In February HHS issued the final rules for enforcement of the HIPAA administrative simplification requirements (see the February 16 *Federal Register*, 71FR8390). While there have been relatively few complaints regarding organizations' approaches to the HIPAA privacy and security rules, regulations for civil and criminal penalties related to HIPAA have been enacted.

Talk on the Hill

Some individuals and organizations want health information, be it generalized or specific to an individual, to be strictly private; others feel they need unlimited access to healthcare data for public health, biosurveillance, research, quality assurance, injury monitoring, and data mining. While access to health information is necessary for the well-being of the public, we must balance this need with the individual's right to privacy.

When HIPAA was passed in 1996, Congress gave itself three years to resolve many of the open issues, otherwise the legislation provided that the HHS secretary would resolve the problems. This is exactly what has happened. Now some in Congress are suggesting that they will go along with RTI International's findings if consensus is achieved on national standards for confidentiality and security within three years. However, if consensus is achieved but no action is taken by Congress, then the HHS secretary will once again be called on to create uniform nationwide standards (i.e., regulations) to eliminate barriers to the NHIN.

While language in the current Health Information Technology Promotion Act (HR 4157) in the House of Representatives calls for this approach, Senate staff has suggested that perhaps the discussion on privacy, confidentiality, and security should wait until next year. As we have noted in past columns, the current session of Congress will effectively terminate early in the summer to allow members to campaign for the fall elections; thus, if privacy does not draw traction soon, it could be the end of discussion for 2006. The issue would be left for another day or for the potential that the individual states might work to achieve consensus without Congress. AHIMA supports the RTI consensus process, with the hope that policy makers will pass the necessary legislation to achieve uniformity across the nation.

Meanwhile, others are asking Congress to address aspects of the privacy issue in another way. A year ago the Senate passed the Genetic Information Nondiscrimination Act of 2005 (S. 306). While the bill does not address all possible discrimination resulting from access to healthcare data, it does address discrimination on the basis of genetic information. It is a complicated bill, because over the years different legislation has provided for such access by a variety of non-HIPAA entities including insurers and employers, and these latter groups have continued to argue against such a bill. While it is not clear if S. 306 can be passed in the House in this short Congressional year, it is clear that more and more consumers agree with the value of sharing their personal health information--so long as they are not discriminated against. If this issue is not resolved, it could prove to be the most significant barrier to health information exchange.

HIM in the Middle of Things

Once again HIM is in the middle of the discussion concerning privacy and security. Discussions will be held in local communities about these issues as the interest and momentum for health information exchange increases. The RTI project will directly affect HIM professionals, since in many cases they can best describe the local legal and business practices behind the study of HIPAA and state laws. AHIMA members are also becoming closely involved with healthcare consumers via discussions about personal health records and privacy.

Confidentiality and security have been key AHIMA issues for many years. HIM professionals have a unique role to help build confidentiality and security into the NHIN by educating the industry, Congress, and healthcare consumers.

Note

1. Department of Health and Human Services. "HHS Awards Contracts to Advance Nationwide Interoperable Health Information Technology." Press release, October 6, 2005. Available online at www.hhs.gov/news/press/2005pres/20051006a.html.

Dan Rode *(dan.rode@ahima.org) is AHIMA's vice president of policy and government relations.*

Article citation:
Rode, Dan. "Privacy and Security in an Electronic Age: E-HIM Environment Poses New Challenges for HIPAA" *Journal of AHIMA* 77, no.4 (April 2006): 18,20-.