Privacy and Security Take Center Stage: Events in May Affect HIM's Privacy and Security Obligations

By Dan Rode, MBA, CHPS, FHFMA

While many HIM issues have been raised this spring, confidentiality, privacy, and security have cast a shadow on all of them, reminding HIM professionals of their data stewardship responsibilities as new rules and requirements are published. Thus in May three events occurred that will affect HIM's confidentiality, privacy, and security obligations.

Disaster Recovery

Tragically, the first event came when a series of natural disasters including floods and tornadoes hit large portions of the country. Certainly the primary concern for those in the affected areas is loss of life, and AHIMA has taken steps to assist fellow professionals as best it can.

In June the AHIMA Foundation established the Health Information Relief Operation (HIRO) Fund to help HIM professionals whose lives and communities have been shattered by natural or man-made events. AHIMA provided an initial donation of $10,000. HIM professionals are encouraged to support the fund and help those in need. To donate, visit www.ahimafoundation.org.

These events also raised concerns about lost health information. The Missouri Hospital Association asked Missouri citizens who find health information to deposit it with their local post office. Other areas may have to undertake this practice as well due to the breadth of the tornadoes' paths.

The Office for Civil Rights (OCR) is also helping those affected deal with this situation. AHIMA is advising OCR on how best to incorporate HIM in disaster recovery efforts.

St. John's Hospital in Joplin, MO, took a direct hit by a tornado. A significant amount of its protected health information (PHI) is stored electronically; however, few if any entities maintaining PHI are prepared for such an event and the aftermath. Communities and organizations should review their disaster recovery plans and update them as necessary to ensure they are prepared for this type of event.

OIG Privacy Security Concerns

In mid-May the Office of Inspector General (OIG) within Health and Human Services (HHS) published two reports citing concerns with how OCR and the Office of the National Coordinator for Health IT (ONC) are responding to the need for privacy and security requirements associated with PHI. OIG's concerns were based on a previous OIG audit that cited a lack of security practices being followed by healthcare providers.

While OIG's audit sample was small, the issues it raised have been brought up in other industry and government circles, especially with the recent push for EHRs and health information exchange. In its public comments on OIG's reports, AHIMA raised concerns that a significant number of healthcare providers were not in full compliance with the HIPAA security regulations.

OIG urged OCR to take a more active role in performing security audits as mandated by the HITECH Act. In 2009 the HHS secretary charged OCR with enforcing HIPAA security requirements, and the HITECH Act called for more audits, though it did not specify additional funding to perform such audits.

OCR responded that it does perform security audits as part of its response to privacy and security complaints and as part of follow-up to breaches. In its report, OIG indicates some skepticism regarding OCR's general security audit process. It remains

to be seen if Congress or HHS will give OCR more funding to perform more audits.

In its report to ONC, OIG "found that ONC had application controls in the interoperability specification, but there were no HIT standards that included general IT security controls." OIG pointed to requirements or criteria ONC could place on EHRs and HIE systems, including encrypting data stored on mobile devices and requiring two-factor authentication for remote access to a health IT system.

Given the fact that OIG's reports were released immediately before the Health IT Committees' recommendations for stage 2 meaningful use requirements, expect to see OIG's privacy and security recommendations included in the stage 2 proposed rule, which is due in the fall. Most of the items identified in OIG's reports have also been raised in recent discussions by the Health IT Committees, especially the Health IT Policy Committee's Tiger Team.

Accounting of Disclosure Rule

It was a surprise when, at the end of May, OCR suddenly released its proposed accounting of disclosure rule. The rule had been awaiting review by the Office of Management and Budget since February, and OCR had indicated at meetings in early May that it would release the other HITECH privacy and security rules this fall.

Many people were even more surprised to find that OCR had included an accounting of access provision in the rule and an approach to utilize the concept of an electronic designated record set rather than the EHR.

The rule is divided into three parts. The first part expands disclosure requirements to cover treatment, payment, and operations information, but only if it is electronic and from the designated record set. The rule also applies to HIPAA covered entities, including business associates.

OCR believes that covered entities should have already determined the systems associated with their designated record set. However, it does define information that would be considered outside of the record set for the purposes of an accounting.

As indicated in HITECH, the proposed rule mandates that organizations provide accountings of disclosures for a three-year period, reducing HIPAA's current requirement of six years. OCR lists the types of disclosures that are subject to the accounting requirement.

The second part of the rule describes a proposal to report access to the electronic designated record set. OCR recognizes that most individuals who request an accounting of disclosure are more interested in who accessed their information.

OCR also realizes that only electronic systems can track access information, and it therefore limits this requirement to information kept in electronic records. Again the accounting would only go back three years.

OCR uses the electronic designated record set because an EHR is not a universally defined set of information and could conceivably consist of a number of different systems. Since the EHR cannot be defined, OCR believes that the designated record set is a much better way to proceed given the changes in EHRs that could be made in the future.

OCR also will work with ONC to coordinate both offices' requirements. AHIMA expects to see this coordination in the stage 2 meaningful use requirements and associated EHR certification criteria.

A number of requirements related to the access report will need to be resolved by diverse covered entities. In addition, the rule's compliance date fluctuates depending on when an electronic designated health record system has been obtained. This presents an interesting situation because it is likely that the designated health record set could be implemented in stages since it likely covers more than one electronic system.

The third part of the rule specifies the supporting requirements for items like revising the notice of privacy practices. These bear consideration since more HIPAA-HITECH requirements are due in the fall.

Over the last month a workgroup made up of members from AHIMA practice councils has been working to respond to the rule and make recommendations for changes. AHIMA expects to release its comments by mid-July. These comments and

other material related to confidentiality, privacy, and security can be found on AHIMA's Advocacy and Public Policy Web site www.ahima.org/advocacy.

Comments on the rule are due to OCR no later than August 1, 2011. HIM professionals should review it for practice and system requirements (present and future) and provide feedback to OCR.

References

Department of Health and Human Services. "HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act." *Federal Register* 76, no. 104 (May 31, 2011): 31426–49.

Office of Inspector General. "Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight." May 2011. http://oig.hhs.gov/oas/reports/region4/40805069.asp.

Office of Inspector General. "Audit of Information Technology Security Included in Health Information Technology Standards." May 2011. http://oig.hhs.gov/oas/reports/other/180930160.asp.

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

Article citation:
Rode, Dan. "Privacy and Security Take Center Stage: Events in May Affect HIM's Privacy and Security Obligations" *Journal of AHIMA* 82, no.7 (July 2011): 16-18.