

HIPAA Security Enforcement Heating Up

Thank you to Advance Magazine for permission to use this article

Leslie: I have heard some buzz recently about security audits. Though the HIPAA security provisions have been in place since April 2005, the first security audit wasn't done until last year. And now I understand that the Centers for Medicare and Medicaid Services (CMS) has contracted with PricewaterhouseCoopers (PWC) to do more security audits in health care organizations this year.

Patty: That's right Leslie; Modern Healthcare reported in January that according to Karen Trudel, deputy director of electronic health standards and services at CMS, under a 1-year contract PWC will conduct compliance reviews of the security programs at 10 to 20 organizations. The reviews will be done at organizations for which CMS has received a complaint.

Leslie: Between these new audits and National Health Information Privacy and Security Week coming up April 13-19, it sounds like there is an opportunity here for HIM professionals, especially those who are also privacy officers, to step up their efforts to further enhance the privacy and security of personal health information (PHI). Though most security officers are IT professionals, I envision that HIM professionals and privacy officers will be collaborating with IT to make sure that all necessary security policies and procedures are in place, that people are aware of them and that they are being followed.

Patty: Let's check in with our own privacy officer, Gwen Hughes, RHIA, CHP, director of e-HIM consulting services at Care Communications Inc. to learn more about this.

Leslie: Great idea. Gwen, what is the role of HIM professionals and privacy officers in assuring compliance with the HIPAA security rules?

Gwen: First, let me say that it is very important for all HIM professionals to be fully versed and involved in the security program of their organizations. Some people think that HIPAA security is narrowly focused on protecting systems from hackers, and that the security of electronic PHI is the bailiwick of the IT department. The potential security vulnerabilities go way beyond the dangers of someone intentionally hacking into electronic systems, however. The HIPAA security rules require physical, administrative and technical safeguards. The best security programs are the result of collaboration by a team that includes IT and HIM professionals at a minimum. Health information security is a responsibility to which HIM professionals have long been committed, and in fact it is part of the American Health Information Management Association's (AHIMA) Code of Ethics.

Patty: Good point Gwen. It is our ethical obligation to help provide leadership in the organization with regard to this issue. The third principle in the Code of Ethics states, "Preserve, protect and secure personal health information in any form or medium and hold in the highest regard the contents of the records and other information of a confidential nature, taking into account the applicable statutes and regulations." So please tell us how our colleagues are going beyond the walls of the HIM department to help their organizations' PHI security programs?

Gwen: Some of our colleagues co-lead the PHI security risk analysis working with IT or a security committee to assess their organization for gaps in security related to access, storage and transmission of PHI. They help prioritize risks and develop action plans to address those risks. One of the apparent risks, for example, is from inadequate physical control of electronic PHI beyond the health organization's campus. Check out the health privacy project Web site (www.healthprivacy.org) for stories in the news about security breaches.

Leslie: There are so many portable devices that are easy to remove from the premises, such as laptops, hard drives, backup media, USB flash drives, PDAs, etc. Portable devices have made it easier to accomplish the work of health care organizations by enabling offsite work, but along with that convenience is the responsibility for users to be more vigilant about protecting the devices and the PHI they contain.

Patty: I know that remote access policies are top of mind for HIM professionals as more and more HIM functions are done offsite, such as remote coding. When we encounter rigorous security practices and excellent security technology, we see HIM and IT working hand and hand.

Gwen: Yes, the HIM directors need to work closely with IT departments on assuring secure access from remote locations, but also on the telecommuting policies and procedures that require their staff or their HIM services contractors to maintain the security of PHI in their remote offices. For example remote location computers should have automatic logoffs for when they might be left unattended for a few minutes, and there should be requirements for keeping the computers or other storage devices in a secure space.

Leslie: What all this says to me is that a lot of people beyond the IT department and HIM need to be aware of and involved in making sure the HIPAA security rules are met. Every department needs to make sure that its policies reflect the organization's commitment to security, and must implement strategies to periodically educate and remind the work force of steps to minimize risk. For example a hospital with a home health care unit needs to make sure that IT, HIM, human resource and clinical departments providing home care adhere to common policies supported by department procedures and that the work force is educated and periodically reminded of those policies and procedures. These policies and procedures would include steps to be taken to protect PHI maintained on laptops traveling with visiting clinicians.

Patty: I agree with that. I think HIM professionals are providing a lot of education and training about security policies and procedures for their own staff as well as for other personnel in the organization. Just as we have always worked hard to keep the awareness of patient confidentiality top of mind in the organization, we now must go further and sound the alarm about the increased risk that security issues pose to our patients' confidentiality in the electronic environment.

Leslie: And let's not forget that the increasing number of incidents and the concern of the public about medical identity theft also underscore the risk inherent in a security breach.

Gwen: HIM professionals are also involved in helping to bridge the gaps found during their organization's risk analysis activities by developing risk management strategies to incorporate into their policies and procedures. As hospitals implement their EHRs, our colleagues also are working on business continuity plans, and many are involved with developing the policies and procedures for role-based access to electronic systems.

Patty: I hope they are including provisions for regularly monitoring compliance with their policies and procedures. It isn't enough to just develop the policies and procedures and educate people. Everyone must know that the organization is totally committed to enforcing their security programs. I am sure that is what CMS will look for when their auditors do security audits.

Gwen: That brings up another good point, Patty. Health care organizations need to have good policies in place for addressing security incidents and non-compliance when it is discovered. How will security breaches be managed? What procedures will be put into place for securing and preserving evidence, for managing the harmful effects of improper use or disclosure, and notifying affected parties? What is the organization's sanction policy and do employees understand the consequences of failing to comply with security policies and procedures?

Leslie: Gwen, as a privacy officer who works closely with the security officer, these rules and the ideas for meeting them seem to just roll off your tongue. For those of us who have been somewhat less involved, what resources do you suggest for those people looking to become more familiar with the rules and the ways for assuring the security of PHI.

Gwen: There are several really good sources. The CMS Web site has excellent educational materials that our readers can access. At www.cms.hhs.gov/SecurityStandard/, readers can find a link to the standard as well as to an educational series of papers on security guidance. For example the one on remote use of and access to electronic protected health information includes an extensive chart of possible risk management strategies. HIMSS has a number of interesting tools. At www.himss.org/content/files/ApplicationSecurityv2.3.pdf for example, they've posted a checklist for evaluating the security features of new software being contemplated. For AHIMA members, the Body of Knowledge at www.ahima.org is an excellent resource for articles on HIPAA security. I should point out that just last month there was an excellent article in the Journal of AHIMA, "How to React to a Security Incident" by the AHIMA 2007 Privacy and Security Practice Council. So there really are a lot of resources available with practical advice.

Also, it's important to be thoroughly conversant in your organization's existing security policies and procedures. This may be a good opportunity to build a closer relationship with the IT department by engaging them in a dialogue about security and the possibility of having to respond to a CMS security audit.

Patty: I understand that CMS will be publishing the results, though not the names of the institutions audited, and the lessons learned about data security issues from the audits. I know we will be watching the CMS Web site for these invaluable updates as another resource.

Gwen: I would also like to add that an article in Computer World last summer, "HIPAA Audit at Hospital Riles Health Care IT" by Jaikumar Vijayan, discussed the concerns raised by the first CMS security audit, which was performed last year. See the article [here](#).

In addition to the concerns hospitals may have about greater enforcement of the HIPAA security rules, the article quoted Peter Mackoul, president of HIPAA Solutions, as saying "increasingly law enforcement authorities and courts are using and interpreting HIPAA in ways that could have broad implications for organizations handling health care data." He cited a case in which the verdict basically allowed the plaintiff to use HIPAA as a "standard of care" to bring an individual action against an organization.

Leslie: Well, all the more reason for HIM professionals to become more active in their health care organizations' security program.

Patty: I would like to thank Gwen for sharing her expertise in this area with our readers. We wish all of our readers a very successful National Health Information Privacy and Security Week, April 13-19, 2008. At www.ahima.org/hipsweek/ you can download suggested activities and documents to distribute to the public or within your organization. It's a great opportunity to promote privacy and security as well as gain visibility in your organization for yourself and the HIM profession.

Leslie Ann Fox is chief executive officer and Patty Thierry Sheridan is president of Care Communications Inc., a national HIM consulting and staffing company headquartered in Chicago. They invite readers to send their thoughts and opinions on this column to lfox@care-communications.com or pthierry@care-communications.com.