Health Law | manatt

May 18, 2011

HHS OIG Audits Uncover Weaknesses in Health Information Security Oversight

Authors: Robert D. Belfort | Helen R. Pfister | Susan R. Ingargiola

On May 17, 2011, the U.S. Department of Health and Human Services' ("HHS") Office of the Inspector General ("OIG") released two audit reports focused on the federal government's health information security activities. The first report assessed the sufficiency of the Centers for Medicare and Medicaid Services' ("CMS") oversight and enforcement of the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule (the "Security Rule"). The second report evaluated the Office of the National Coordinator for Health Information Technology's ("ONC") adoption of technology standards to protect the security of health information in health information technology ("health IT") tools.

OIG released the reports amid a flurry of recent federal information privacy and security activity, including the White House's release of a draft "National Strategy for Trusted Identities in Cyberspace," which calls for the creation of an "identity ecosystem" to protect electronic data, including health and financial information. The ecosystem would reduce the need for passwords and logins by providing people with a secure, interoperable digital identity. HHS is also reportedly close to releasing an "omnibus" final regulation amending HIPAA in accordance with the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

OIG's Assessment of CMS's Oversight and Enforcement of the HIPAA Security Rule

Between October 2008 and March 2010, OIG conducted one audit of CMS's Security Rule oversight and enforcement activities (which it performed at CMS headquarters in Baltimore, Maryland) and seven audits of hospitals' Security Rule compliance (which it performed at hospitals in California, Georgia, Illinois, Massachusetts, Missouri, New York, and Texas).

Combining its findings from the audits and releasing them in a single "nationwide roll-up review," OIG found CMS's oversight and enforcement actions insufficient to ensure that HIPAA Covered Entities (i.e., health plans, health care clearinghouses, or health care providers that transmit any health information in electronic form) effectively implemented the Security Rule. According to OIG, "CMS had limited assurance that controls were in place and operating as intended to protect [electronic Protected Health Information ("ePHI")], thereby leaving ePHI vulnerable to attack and compromise."

Background The Security Rule requires Covered Entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting ePHI. Specifically, Covered Entities must:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

CMS had authority to enforce the Security Rule until July 2009, when HHS transferred that authority to the Office for Civil Rights ("OCR").

Common Security Vulnerabilities OIG's audits of seven hospitals identified 151 vulnerabilities in the hospitals' systems and controls to protect ePHI. OIG categorized 124 of them as "high impact." Examples include the following:

- *Wireless Access Vulnerabilities*: These included ineffective encryption and lack of authentication to enter a wireless network, among others.
- *Access Control Vulnerabilities*: These included inadequate password settings, computers that did not log users off after periods of inactivity, and unencrypted laptops containing ePHI, among others.
- *Audit Control Vulnerabilities*: These included disabled audit logging, among others.
- *Integrity Control Vulnerabilities*: These included uninstalled security patches and outdated antivirus updates, among others.
- *Person or Entity Authentication Vulnerabilities*: These included inappropriate sharing of administrator accounts and unchanged default user identifiers and passwords.
- *Transmission Security Vulnerabilities*: These included lack of email encryption and unsecure network services, among others.
- *Facility Access Control Vulnerabilities*: These included unsecured physical access to ePHI in data centers.
- *Device and Media Control Vulnerabilities*: These included lack of inventory systems to track computer equipment containing ePHI, among others.
- *Security Management Process Vulnerabilities*: These included incomplete risk assessments and lack of policies and procedures for risk analysis.

- *Workforce Security Vulnerabilities*: These included employee user accounts with inappropriate network access and delayed deactivation of terminated employees' network access.

- *Security Incident Procedure Vulnerabilities*: These included lack of procedures to identify, respond to, or document actions taken in response to security incidents.

- *Contingency Plan Vulnerabilities*: These included incomplete contingency plans, incomplete disaster recovery plans, unsafe storage of backup tapes, and network security disruptions.

OIG's Recommendations In its audit report, OIG recommended that OCR continue the compliance review process begun by CMS, and that it implement procedures for conducting compliance reviews, even in the absence of complaints. In its response, OCR noted that it maintains a process for initiating compliance reviews of Covered Entities, and that it had performed compliance audits on Covered Entities that had suffered breaches involving records of more than 500 individuals—the threshold for an organization to report to the government for posting on its public breach notification list. According to OIG, while OCR may maintain a process for initiating Covered Entity compliance reviews in the absence of complaints, it provided no evidence that it has actually used that process, except in response to reported security breaches. In short, OIG asserted that OCR needs to do more.

OIG's Assessment of ONC's Health IT Security Standards

Under the HITECH Act, ONC is charged with developing a nationwide health IT infrastructure that allows for the electronic use and exchange of health information. The HITECH Act required ONC to adopt standards, implementation specifications, and certification criteria for electronic health records ("EHRs") used by health care providers participating in the Medicare and Medicaid EHR

Incentive Programs. ONC released interim final and final rules adopting an initial set of standards, implementation specifications, and certification criteria in January 2010 and July 2010, respectively.

OIG's objective in auditing ONC was to "assess the IT security controls" in ONC's initial set of standards. In its audit report, OIG differentiated between two types of security measures. One it described as "application security controls" that "function inside systems or applications to ensure that they work correctly." An example is a requirement that EHRs be able to encrypt data shared between providers. The other it described as "general information technology security controls," which are "structure, policies and procedures that apply to an entity's overall computer operation." An example would be a policy that requires providers to use encryption software on their systems (i.e., when data is at rest) and encrypt all data copied from an EHR and placed on a portable storage device, such as a laptop, CD, or a portable thumb drive

Federal Health IT Standards Short on General IT Security Controls After reviewing ONC's initial set of standards, OIG found that the standards included security features necessary for securely passing data between EHR systems (e.g., encrypting transmissions between EHR systems) but lacked "general IT security controls." In addition to the encryption example noted above, OIG cited two other general IT security controls, the absence of which it found problematic. These included requiring two-factor authentication when remotely accessing a health IT system, and patching the operating systems of computer systems that process and store EHRs.

OIG noted that it found a lack of these and other general IT security controls during prior OIG audits of Medicare contractors, state Medicaid agencies, and hospitals. According to OIG, these vulnerabilities "raise concern about the effectiveness of IT security for [health IT] if general IT security controls are not addressed."

Concern that HIPAA May Not Provide Adequate General IT Security According to OIG, the lack of general IT security controls in ONC's initial health IT standards reflects ONC's position that the Security Rule provides adequate general IT security, and that more specific requirements need not be imposed on health IT tools or on the users of those tools – at least not yet.

OIG disagreed with this position, stating that vulnerabilities in HHS's oversight of and Covered Entities' compliance with the Security Rule make relying on HIPAA to protect health information included in health IT tools a risky strategy – even for now. Further, it should be noted that the Security Rule does not mandate that Covered Entities encrypt data at rest on their computer systems, nor that they install security patches. It also does not specify the type of authentication protocol Covered Entities should implement to ensure the security of their patients' health information.

OIG's Recommendations In its audit report, OIG recommended that ONC:

- Broaden its focus from interoperability specifications to include well-developed general IT security controls for supporting systems, networks, and infrastructures;
- Use its leadership role to provide guidance to the health industry on established general IT security standards and IT industry security best practices;
- Emphasize to the medical community the importance of general IT security; and
- Coordinate its work with CMS and OCR to add general IT security controls where applicable.

ONC concurred with OIG's recommendations, and, in its response, provided an overview of its "extensive portfolio of initiatives (that are completed, in process, or in the planning and formulation stages) that seek to promote increased security

and the public's trust in health IT and electronic health information exchange." ONC noted that it has "worked to strike the right balance between ensuring the security of health information among new adopters while not creating such an onerous burden of technical requirements that the primary adoption goal would fail to be achieved," and that it is committed to a strong security framework in the future.

Key Takeaways from the OIG Audits

Covered Entities and others using EHRs under the Medicare and Medicaid EHR Incentive Programs should keep a close eye on federal health IT standards and HIPAA enforcement activities. Improved compliance with existing Security Rule requirements and an ability to adapt to new, potentially stronger general IT security standards for health IT tools (such as two-factor authentication) could be integral to securing patients' health information in the future.

back to top