

OIG Launches Audits of Hospital Compliance With HIPAA Security Rule

Reprinted from the March 8, 2007, issue of [MEDICARE ADVANTAGE NEWS](#), biweekly news and analysis on the Medicare (and Medicaid) managed care programs.

With the HHS Office of Inspector General (OIG) starting HIPAA security compliance audits — and given other security threats out there — it's a good time for covered entities to assess the state of their security practices and the documentation that guides them. Consider starting with the matrix at the back of the HIPAA security regulation because it's a good bet that OIG auditors are using it to evaluate compliance, one expert says.

In a surprise move, OIG on March 5 began the first audit of a provider's compliance with the HIPAA security regulation. The target: Piedmont Hospital in Atlanta. Auditors are expected to stay at the hospital three to four weeks and then forward their findings to CMS, which enforces the security rule.

This is the government's first systematic hands-on examination of compliance with any HIPAA regulation. The HHS Office for Civil Rights (OCR) has been enforcing the privacy rule for several years, but it acts on complaints and then either helps cooperative covered entities correct their violations or refers egregious cases to the Department of Justice for potential criminal prosecution. CMS enforces the security regulation as well as the transaction and code sets regulation, but so far there haven't been formal audits. Four people have been convicted of HIPAA crimes, but there have been no civil fines. And now, with no fanfare, come the Medicare watchdogs.

OIG Region 4 in Atlanta is kicking off the first provider HIPAA security rule audit, but a source indicates it will be national. Some Medicare fiscal intermediaries have also been audited by OIG for HIPAA security rule compliance, says the source, who has direct knowledge of the audit but declines to be identified.

An OIG spokeswoman says, "We can't answer questions about ongoing work. The number of audits to do has yet to be determined."

OIG auditors plan to audit Piedmont's administrative, physical and technical safeguards — the core requirements under the security regulation. This will include the hospital's policies and procedures relating to access to electronic protected health information (e-PHI); the risk assessment relative to e-PHI; electronically transmitting e-PHI; preventing, detecting, containing and correcting security violations; monitoring systems; remote access; wireless security; anti-virus mechanisms; firewalls; and other e-PHI security requirements.

It appears that Piedmont had relatively short notice from the OIG auditors of the upcoming security audit, the source says.

The security regulation mandates physical, technical and administrative safeguards for e-PHI, brought to life through certain standards. For every standard, the security rule provides a number of "implementation specifications." There are two kinds of implementation specs: required and "addressable."

Required obviously means the covered entity must do it. Addressable, however, is not the other extreme; it's not optional. But there's some wiggle room here. If an implementation specification is addressable, then the covered entity can assess whether it is a reasonable and appropriate safeguard for the covered entity. It can be tailored to an organization - an attempt by HHS to build in some flexibility for a very diverse industry - or can be bagged altogether if the covered entity documents why and substitutes an equivalent measure to meet the same security standard.

Get Up to Snuff

In the face of a possible OIG audit and generally given the potentially disastrous consequences of a breach, organizations should take a hard look at their level of security compliance, says consultant Chris Apgar, president of Apgar & Associates LLC in Portland, Ore.

First stop: policies and procedures. He says they should be "accurate, complete, communicated [to employees and others] and enforced." OIG, he says, will look at what is in writing in terms of physical, administrative and technical safeguards.

But after OIG auditors assess the documentation, they will want to see concrete proof that the organization is putting its money where its mouth is. For example, OIG will delve into the management of anti-virus software, says Apgar, a certified information systems security professional.

What is the package you are using? Show me. Do you periodically update signature files, and how do you do that? How often do you run virus scans to catch anything bad from outside (e.g., an employee brings in an infected game from home)?

What about your transmission of information? Are you sending PHI across the Internet unsecured, or encrypting it? While encrypting e-mail was an addressable specification, at this point Apgar thinks anything but encryption would be hard to justify because encryption software ranges from dirt cheap for small organizations to higher in cost for medium to large organizations.

OIG may also look at sanctions policies. Are they strong? Are they enforced? What about your disaster recovery plan? The security rule requires contingency planning so that the critical mission of the organization can continue even if the building is destroyed.

"OIG will probably have a checklist they march through," Apgar says. He is betting on the matrix at the end of the security regulation.

It focused on ways that organizations could protect e-PHI when it's used or accessed offsite.

Risk Assessment: More Than Once

Apgar says the "foundation of any security program is the risk assessment or analysis. It's a required element of the security rule." Do a risk analysis annually or "when any significant technology or business change (e.g., a merger) occurs." Then follow the risk assessment with risk management: Deal with the risks identified in the risk assessment and follow through to make sure the problems that need to be addressed were actually corrected. "Lots of organizations did an initial risk assessment and then never did anything again," Apgar asserts.

But risk management doesn't mean fixing every threat identified. Organizations should prioritize their risks. For example, suppose you have an extensive network security program in place. It's governed by policies and procedures and has firewalls and an intrusion detection system, and it's properly manned. No system is flawless, but the risks it presents (e.g., hackers, damage due to a specific type of natural disaster, etc.) are low, so the decision is made not to beef it up.

Threats can be ranked quantitatively, which is more mathematically based, expensive and time-consuming, or qualitatively, which is more subjective but practical. With the quantitative method, you can evaluate identified threats and vulnerabilities in a simple table. Across the side, put low, medium and high, representing the possibility that the threat will happen or the vulnerability will be exploited. Across the top, put the damage to the organization if it does occur - low, medium or high.

For example, one risk would be the damage to the organization if the anti-virus software isn't updated. Can the organization be exploited? The answer is "yes." Would the damage be low, medium or high? The answer: high. That means action must be taken. Employees must be educated not to open attachments from people they don't know, the anti-virus software must be updated, policies must be rewritten requiring routine updating of anti-virus software, etc.

Regular audits are also mandated in the security rule. "It's part of the security rule to log certain events and review those logs regularly," Apgar says. Most software applications can automatically create a record every time Joe Smith accesses Betty Jones' PHI as long as the audit log built into the software is activated. Organizations should periodically look at these audit logs to make sure an access was not improper or initiate an investigation when specific suspicions arise, he says. Also, organizations should conduct an organized general audit at least annually just like your annual financial audit.

This first provider audit comes on the heels of CMS's publication of industry guidance on implementing the security regulation. In January, CMS issued the "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information (E-PHI)," which was crafted mainly to reiterate some ways that covered entities "may protect e-PHI when it is accessed or used outside of the organization's physical purview."

View the CMS HIPAA security guidance on e-PHI at www.cms.hhs.gov/SecurityStandard.