HIPAA audits have begun [Lawyers USA]

Publication Date 12/15/2011
Source: Lawyers USA

HIPAA audits have begun [Lawyers USA]

All entities covered under the Health Insurance Portability and Accountability Act must get ready - audits of privacy and security compliance under the Act have officially begun.

Under the auspices of the 2009 HITECH (Health Information Technology for Economic and Clinical Health) Act, the Department of Health and Human Services was mandated to conduct periodic audits to ensure HIPAA compliance.

Prior to HITECH, HHS investigated potential HIPAA violations based on specific complaints.

The new audits will impact all types of covered entities, which will need to supply auditors with documentation and host an on-site visit.

Calling the initial round of audits a "pilot program," the Office for Civil Rights (OCR) said the focus is on prevention and education rather than penalizing covered entities. The audits will be completed by December 2012, and HHS will share best practices learned from the audit process and provide guidance based on the shortfalls found.

But entities with particularly egregious noncompliance could face further investigations or monetary penalties, according to Adam H. Greene, a partner in the Washington, D.C. office of Davis Wright Tremaine who formerly worked at the OCR and focuses his practice on HIPAA compliance.

"I don't expect too many, if any, covered entities to come out of this audit-proof," he said. "Some segments [of covered entities] are fully aware of the audits, but others - like small medical practices - are not aware. There are a lot of covered entities that are unprepared for an outside audit."

Joseph Lazzarotti, a partner at Jackson Lewis in White Plains, N.Y., agreed.

"In my view, no one is 100 percent compliant," he said. With regulations being updated or added frequently and the technology constantly changing, "the ground of compliance is always shifting and it is hard to keep up."

The audit process

To help guide covered entities, the OCR has issued guidance about the process of the audits.

* Who will be audited?

Between now and December 2012, a total of 150 covered entities will be audited. While there was some question as to whether the "business associates" of covered entities would also be audited, OCR has indicated that they will be audited "in the future."

"My interpretation of that statement is that business associates will not be targets for the first 150 audits," Greene said.

OCR has also stated that the audits will cover a broad range of entities, both large and small. All three types of covered entities - health care providers, health plans and health care clearing houses - will be audited, Greene said.

"And I expect all different types of health care providers will be audited, like general hospitals, specialty care hospitals, large group practices, small practices and pharmacies," he added.

* What does an audit entail?

The audit process will begin with a notification letter that contains a preliminary request for documentation. Covered entities may receive as little as 10 days to provide that documentation, which will be followed by an on-site visit that could last anywhere from three to 10 days, depending on the complexity of the organization.

Auditors will focus on two things, according to Greene: interviews with employees and looking at routine operations to determine whether they are consistent with the entity's policies and procedures and the regulations themselves.

"It could be everything from looking at servers and work stations to checking locks on cabinets," he said.

While the OCR has indicated that only high-level staff will be interviewed (such as a privacy officer, Chief Information Officer or general counsel), lower-level staff could be questioned as part of the review of routine operations, Greene speculated.

Auditors are likely to ask employees questions like, "What is the policy on X?" or "Where is the policy located?" said Amy Fehn, a partner at Wachler & Associates in Royal Oak, Mich.

* What happens after the audit?

If a covered entity passes an audit with flying colors, the process ends. But given the complexity of HIPAA's privacy and data security requirements, such perfect compliance is unlikely, Greene said.

If there are minor adverse findings, HHS will work with the covered entity to take steps toward appropriate, corrective action. However, if the audit reveals serious noncompliance, "that could lead to a formal enforcement action, such as a settlement agreement with a corrective action plan or a civil monetary penalty," Greene said.

OCR will not release a list of the audited entities or specific findings, but will issue an aggregated report of the final results of the audits, Lazzarotti said.

Preparation for an audit

In preparation for an audit and to achieve compliance with HIPAA, covered entities must have "an appropriate set of policies and procedures in place," said David Harlow, a health care attorney at The Harlow Group in Newton, Mass. and author of the HealthBlawg.

A system of training and re-training employees should also be established, Harlow said.

Fehn said training should occur on an annual basis at a minimum, with immediate training for new hires.

"Every time a training is performed - under both the privacy and security regulations - have a sign-in sheet and keep those in a file to document who was there and that the training occurred," she advised.

Ensure that any existing systems are maximized to their full capability, Fehn added.

"For example, if an entity has settings that log employees off after a certain time period, make sure that function is turned on and is being used," she said.

Harlow recommends encrypting electronic health records, although he acknowledged opponents' argument that it can be cumbersome and get in the way of day-to-day operations.

"Another approach might be to encrypt certain elements of the record and not the entire record," he suggested, or entities might require portable devices to be password-protected. That way, if a laptop is lost or stolen, its data cannot be read.

"Each covered entity needs to make a judgment about what works best for their organization," Harlow said.

Greene suggested that covered entities focus on potential high- impact vulnerabilities and perform a self-assessment on both the privacy and data security rules.

"Until you have gone around and talked to randomly selected staff or checked the locks on filing cabinets through the organization, you really do not have a good idea if compliance is being achieved," he said. "And better you find out than an auditor."