Health Information Compliance Alert

HIPAA: Take These Steps to Protect Yourself During HIPAA Audits

Contact experienced outside counsel immediately our experts advise.

Establishing HIPAA protocols isn't a one-time job. Make sure your privacy and security practices are up-to-date to account for new information management applications and systems or state laws (i.e., the Massachusetts privacy regulations), or you could come up short under audit, warns **Kenneth Rashbaum, Esq.** of Rashbaum Associates in New York.

"Privacy rules essentially demand that we remain vigilant thus it forces us to always evolve, reach for a standard of excellence, and improve with time," says **Ester Horowitz, CMC, CITRMS, CIISA**.

HIPAA Audits Announced

"The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this mandate, OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance. Audits conducted during the pilot phase will begin November 2011 and conclude by December 2012," according to an HHS press release.

The pilot audit program is a three-step process according to the press release. The first step, which was initiated in July, developed the audit protocols. The initial audits began in November and tested the protocols. The OCR expected these results to modify how the remaining audits were going to be conducted, the HHS said in the release.

"The last step will include conducting the full range of audits using revised protocol materials. All audits in this pilot will be completed by the end of December 2012," according to the press release.

Note: You can read up for further details at www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

Who Will Be Audited?

Technically all covered entities and their business associates are eligible for an audit. The "OCR will audit as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit," the HHS website clarifies. "Business associates will be included in future audits."

"The new program is a random program, and the selection is not dependent on any prior behavior, violations, breaches or any other factor, so there is no way to take action to prevent being audited under this program," says **Jim Sheldon-Dean**, Director of Compliance Services for Lewis Creek Systems in Charlotte, Vt. There will be up to 150 audits performed by the end of 2012 under this particular program, he added.

There are also audits being performed as a result of complaints or breach reports, outside of this new program, resulting in violations and settlements for fines.

What You Can Expect

The OCR will notify you in writing if you are going to be audited and who your audit contractor will be. The audit process will be outlined and requests for relevant documents and other information will be made at this stage to ensure you are prepared for the audit. How and when you should return the requested information to the contractor will be specified at this stage.

Keep in mind: You will have to return this information within 10 business days of receiving the notice. Also, "OCR expects to notify selected covered entities between 30 and 90 days prior to the anticipated onsite visit," according to the website. "In this pilot phase, every audit will include a site visit and result in an audit report. During site visits, auditors will interview key personnel and observe processes and operations to help determine compliance."

What You Need To Do

Put together your documentation of whatever steps you have taken to be compliant with HIPAA and HITECH requirements. "I've seen many organizations big and small lapse in their mitigation and monitoring response. Specifically that they do not review periodically," says Horowitz. Organizations followed HIPAA initially from a system wide approach, she adds. New procedures were adopted and others revised. Many of the procedures from that time continue today but some have become outdated or lax.

Every organization is required to periodically review their privacy policies, procedures, and methodologies and to document that they did, points out Horowitz. Included in these reviews is a demonstration that employees were and are trained, not just one time but also periodically.

"In an effort to standardize and make habit a routine that allows the company to deliver care or support care, it must also be acknowledged that routines become obsolete, need adaptation, updating, and should be minimally reviewed," insists Horowitz. "I do not see that occurring at this stage of the HIPAA life cycle across a majority of organizations."

Remember: Following the site visit, auditors will develop and share with the entity a draft report. Audit reports generally describe how the audit was conducted, what the findings were and what actions the covered entity is taking in response to those findings, the HHS says on its website. Prior to finalizing the report, the covered entity will have the opportunity to discuss concerns and describe corrective actions implemented to address concerns identified.

You should "see it [taking corrective action] as valuable labor ... (and) clearly understand that it is a profit center method that will only elevate the organization's reputation and output if followed and measured appropriately," Horowitz advises.