Health Information Compliance Alert

HIPAA: Don't Wait for Official Notification to Get Your HIPAA Audit Prep Started

The protocols are your road map to solid preparation.

You need to be ready before you get the notification letter that you are up for a HIPAA audit. Focus on these strategies from industry experts to help you prepare before the auditors come knocking.

Get to Know the HIPAA Audit Protocols

The **U.S. Department of Health and Human Services** (HHS) **Office for Civil Rights** (OCR) released detailed HIPAA audit protocols, which audit contractor **KPMG** used during the first round of random HIPAA audits.

"The protocols offer some surprising indications of government enforcement priorities and provide a fairly granular 'road map' of HHS OCR's interests," according to **Ober Kaler** Attorneys at Law's Healthcare Information Technology and Privacy Blog.

The HIPAA audit protocols cover the following requirements:

A. Privacy Rule;

- Notice of Privacy Practices (NPP) for protected health information (PHI)
- Rights to request privacy protection for PHI
- Access of individuals to PHI
- Administrative requirements
- Uses and disclosures of PHI
- Amendment of PHI
- Accounting of disclosures.

B. Security Rule;

- Administrative safeguards
- Physical safeguards
- Technical safeguards.

C. Breach Notification Rule;

- Notification
- Risk assessment
- Timeliness.

"It's nice having the HIPAA Audit Protocol out there because now you have some idea of what sort of things you need to have prepared if you're going to be audited," notes HIPAA expert **Jim Sheldon-Dean,** founder and director of compliance services at **Lewis Creek Systems, LLC** based in Charlotte, Vt.

Tight timeframe: This is especially true since you have very little time to prepare after you've received notification that you'll be audited. You basically have a three-week notice to turn over all the information the auditors want to see.

"And if you're not ready when you get the letter, it's too late. You can't make it after that," Sheldon-Dean laments. "[The auditors] only want to see that something has been prepared before you get the letter."

Best bet: Studying the questions and areas that the HIPAA auditors cover will help you to get ahead of the game, Sheldon-Dean says.

Document Your Compliance Efforts

HIPAA auditors want to see tons of written records of your HIPAA compliance. "Documentation is absolutely essential; you have to have [it] in place," Sheldon-Dean warns.

"Unsurprisingly, the protocols demonstrate a clear bias towards extensive documentation, both in terms of written policy documents and in terms of documentation of risk assessments, compliance activities, training programs, and even documentation of decisions not to take certain compliance or security steps," Ober Kaler stated.

Review, Train, Repeat

Auditors want to see that you're reviewing your policies and procedures often, updating them when necessary and following those updates with staff training. Each and every HIPAA-related policy, form or process should be a "living document."

Pay attention: "The protocols also make regular reference to an entity's obligation to regularly review and update policies (formal or informal) and the obligation to retrain workforce following any change to existing policies (especially with regard to security protocols)," according to Ober Kaler.

Stick to a Policy

"[Auditors] were looking to see how well the organization sticks to its policies, whatever they are," Sheldon-Dean says. For example, you likely have a policy that all staff members must attend HIPAA trainings. But if even one employee misses a training session, auditors can cite that as a deficiency.

Bottom line: "The point is, if you have a policy, you had better be sure you're doing what it says you do, or you will have to defend your actions, and that's just plain expensive, time consuming and unpleasant," Sheldon-Dean cautions.

Ramp Up Your Internal Auditing

In the first round of random HIPAA audits, auditors found that covered entities "weren't doing much internal auditing of system and network activity to ensure proper use of systems and data by the appropriate people," Sheldon-Dean says. "If you haven't started to follow up on the HIPAA Security Rule's system monitoring and activity review safeguards, you're leaving yourself open to fines and corrective actions plans."

Case in point: On May 13, OCR executed a $400,000 settlement with **Idaho State University** (ISU) after the ePHI of nearly 17,500 patients of its outpatient clinics was compromised. ISU self-reported the breach after it realized that the ePHI was unsecured for 10 months due to disabled firewalls on its computer servers.

More specifically, OCR determined that ISU didn't have proper security measures and policies in place to address risks to ePHI, nor did the organization have procedures in place to routinely review their IT system so that it would've detected the breach much sooner.

"Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program," OCR director **Leon Rodriguez** said in a May 21 HHS press release. "Proper security measures and policies help mitigate potential risk to patient information."

Resource: To view the HIPAA audit protocols, visit www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.