Part B Insider (Multispecialty) Coding Alert

Patient Privacy: HIPAA Audits to Scrutinize the Fundamentals of Your Privacy Plans

Ensure that your program discusses how to cover these details to prep for an audit.

Do you know how to de-identify a patient's protected health information (PHI)? Will you be prepared to restore PHI after a data loss? These questions among many others will be on auditors' minds as they audit practices' HIPAA policies this year.

Background: As most practices are aware, the Office of Civil Rights (OCR) has launched phase two of the HIPAA audits, which means that auditors will be reviewing the privacy practices of covered entities (CEs) and business associates (BAs) this year (see the Insider, vol. 17, no. 12 for more).

The OCR recently published its current Audit Protocol on the HHS website, and it offers an in-depth look into what you should be preparing to share if you are selected as an auditee. The protocol shares specific questions that CEs and BAs should ask themselves in preparation for the audits and if you cannot answer any of these questions, it's time to look deeper into your policies, because the auditors will ask you the same questions when they visit

Here's How to Use the New Guidance

When you first bring up the OCR's Audit Protocol document, you may find it slightly overwhelming, since it is very long and includes statute numbers, but if you turn your attention to the chart's fifth column, you'll find the information you need.

"The part that's helpful is the Audit Inquiry column because that column identifies the documents and information that OCR auditors will request and the other columns just restate what's in the Privacy Rule, Security Rule or Breach Notification Rule," says **Daniel F. Gottlieb, Esq.,** a partner with McDermott Will & Emery's healthcare practice in Chicago. "The Audit Inquiry section has the new guidance, and for a small medical practice, to the extent that it has time to read through it, I think it's useful to at least read through that part," he says.

In particular, if you have performed self-audits or you've had an outside source review your HIPAA implementation activities and you are therefore aware of any gaps in your HIPAA compliance program, check the Audit Protocol for questions that will be asked about that area and do your best to ensure that you can show that you have addressed the gaps consistent with OCR's expectations.

In addition, it's a good idea to ensure that your HIPAA compliance program adequately addresses the areas where the OCR will most likely focus its investigations. "Findings that came out of the phase one audit program and recent enforcement activities reveal what OCR will focus on and those have the greatest enforcement risk," Gottlieb advises. "For example, a lot of CEs audited in phase one didn't have (in the OCR's view) an appropriate security risk assessment including a comprehensive assessment of risks and vulnerabilities to ePHI under the Security Rule, and that's an area to focus on. That section of the new Audit Protocol shows what OCR will be asking practices in that area."

Prepare Now Based on the Protocol

If you find that the Audit Protocol indicates that auditors will ask whether you have a particular document on-hand and you don't, it's time to create it, identify an appropriate alternative document or determine that the document is not required by the HIPAA regulations for your practice, Gottlieb advises.

For example, the document indicates that you should have policies and procedures in place to restore any lost data as

well as a disaster recovery plan. If you haven't yet created these protocols, now is the time to act. "Practices should have procedures in place outlining what they'd do in the event of a disaster or other system outage," Gottlieb says. "Most people initially focused on confidentiality and preventing unauthorized access to PHI, but the Security Rule also requires safeguards to assure availability of electronic PHI to authorized users and that's why it impacts your disaster recovery plan and backup protocols."

Don't panic: If you read the entire Audit Protocol, chances are high that you may find areas that you haven't yet addressed, but that doesn't mean you should sound the alarms. "Practices should take care of any gaps now, but the good news is that implementation is scalable," Gottlieb says. "The Security Rule and Audit Protocol indicate that the OCR will take into account the size and capabilities of the organization. It will have greater expectations for a large hospital system than a for a small medical practice."

Resource: To read the complete Audit Protocol, visit www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.