Codify
BY AAPC

Health Information Compliance Alert

HIPAA Audits: Get Ready For Phase 2 Of OCR Audits: Take 7 Steps

Beware: These new audits could lead to civil money penalties.

Now that the Phase 1 audits have finished, the **HHS Office for Civil Rights** (OCR) is poised and ready to begin the second round of HIPAA audits. Are you prepared for OCR to knock on your door for a Phase 2 audit?

What to Expect in Phase 2

Unlike the Phase 1 pilot audits that OCR conducted in 2011 and 2012 which focused on covered entities (CEs) only, the Phase 2 audits will involve both CEs and business associates (BAs), according to **McDermott Will & Emery** (MWE) attorneys in a July 29 article published in The National Law Review.

"Unlike the Phase 1 audits, OCR will conduct the Phase 2 audits as desk reviews with an updated audit protocol and not on-site at the audited organization," MWE noted. And OCR will post the Phase 2 audit protocol on its website so you can use it for your internal compliance assessment.

OCR itself will conduct the Phase 2 audits and will focus on more high-risk areas, explained partner attorneys **Adam Greene** and **Rebecca Williams** in a recent advisory from the law firm **Davis Wright Tremaine LLP**. OCR may also potentially integrate the audits into its formal enforcement program.

This means that if "an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited organization that could lead to civil money penalties," MWE warned.

Pay Close Attention to These Compliance Areas

And in the Phase 2 audits, OCR will target HIPAA standards with the highest numbers of noncompliance in the Phase 1 audits (see "Curious? Find Out What Phase 1 OCR Audits Revealed" on page 60 for more details). According to MWE, these standards include:

- Risk analysis and risk management;
- Content and timeliness of breach notifications;
- Notice of privacy practices (NPP);
- Individual access;
- Privacy standards' reasonable safeguards requirement;
- Training to policies and procedures;
- Device and media controls; and
- Transmission security.

HIPAA compliance experts offer the following steps that you should take to prepare for Phase 2 of the OCR audits:

1. Double-Check Your Risk Analysis

Make sure that your organization has recently completed a comprehensive assessment of potential security risks and vulnerabilities, MWE advised. Also, "confirm that all action items identified in the risk assessment have been completed or are on a reasonable timeline to completion."

What's more: Your risk analysis should actually identify and categorize risks as low, medium or high, "rather than merely documenting that controls are in place or documenting the gaps in compliance with the Security Rule," Greene and Williams urged.

2. Update Your Policies And Procedures

Auditors will also scrutinize your policies particularly your breach notification, risk analysis and risk management policies, as well as your NPP and patient access policies, Greene and Williams noted.

Make sure your organization has implemented a breach notification policy that accurately reflects the content and deadline requirements under the breach notification standards, MWE stated. And check to ensure that your NPP is compliant and not only a website privacy notice.

Additionally, review your organization's HIPAA security policies to identify any actions that you have not yet completed as required, MWE recommended. Review your physical security plans, disaster recovery plan, emergency access procedures, etc.

3. Locate Your Documentation for Quick Access

Because auditors will ask for a plethora of information and documentation and you'll have only two weeks to respond to OCR's audit data request you should keep certain other papers handy. For instance, know how to readily collect documentation of patients' receipt of NPP acknowledgements and, where there is no patient acknowledgment, documentation supporting the reason why you did not obtain an acknowledgement, Greene and Williams said.

Smart idea: Greene and Williams also recommended that you should keep certain supplemental documentation readily available and clearly labeled. This documentation should include breach investigations and risk assessments, risk analyses, and risk management plans, as well as responses to patient requests.

4. Keep a Current List of BAs

Yet another piece of information that auditors will want is a list of your business associates (BAs), so ensure that you have a complete inventory of your organization's BAs for purposes of the Phase 2 audit data requests, MWE said.

Best strategy: You should maintain a current list of BAs with relevant contact information, Greene and Williams agreed. "An internal audit of accounts payable may help identify BAs and is a methodology that was used by OCR's contractors in Phase 1 audits."

5. Check Your 'Addressable Implementation Standards'

Don't overlook: If your organization "has not implemented any of the security standards' addressable implementation standards for any of its information systems, confirm that the organization has documented: (i) why any such addressable implementation standard was not reasonable and appropriate; and (ii) all alternative security measures that were implemented," MWE recommended.

6. Inventory All Your Information System Assets

Confirm that your organization maintains an inventory of information system assets, including mobile devices (even in a bring-your-own-device environment), MWE said. Also make sure that all systems and software that transmit electronic PHI (ePHI) employ encryption technology or that you have documentation in your risk analysis supporting the decision not to employ encryption.

7. Review Your Security Plan

Ensure that your organization "has adopted a facility security plan for each physical location that stores or otherwise has access to PHI, in addition to a security policy that requires a physical security plan," MWE advised. Your organization must have "reasonable and appropriate safeguards in place for PHI that exists in any form, including paper and verbal PHI."