Upcoming HIPAA audits may target financial institutions—here's how to prepare

Much like a tornado watch, the conditions appear to be right for a coming storm: the upcoming Phase 2 HIPAA audits. The Department of Health and Human Services Office for Civil Rights (OCR) has begun verifying contact information of potential audit targets. This serves as a warning that OCR will be auditing for HIPAA compliance, which unlike the pilot audits, will target business associates, including financial institutions, as well as HIPAA-covered entities.

Government regulation is not new to financial institutions. What is new is that an additional regulator with a different perspective has been thrown into the mix. And the stakes are high, with HIPAA carrying both civil and criminal penalties, and resolution amounts tending to reflect the size of the organization being scrutinized.

Financial institutions usually enjoy a statutory exemption from HIPAA when they provide "typical" banking services such as processing payments and issuing credit, even when the financial institutions come in contact with protected health information. But, when services go beyond these recognized functions, financial institutions that create, receive, maintain, or transmit protected health information may well have become business associates with direct obligations under HIPAA (as well as contractual obligation through "business associate contracts"). Additionally, financial institutions that convert non-standard electronic HIPAA transactions (usually transactions related to health care billing and payment) into standard transactions—and vice versa—may be health care clearinghouses that are covered entities under HIPAA.

Preparation for Audits

To prepare for the next round of audits, which is described in more detail below, financial institutions that are business associates or covered entities may want to consider the following steps:

- Verify that a current HIPAA risk analysis is in place and that the risk analysis actually identifies and categorizes risks (e.g., low, medium, high) rather than merely documenting that controls are in place or documenting the gaps in compliance with the HIPAA Security Rule (see OCR Guidance on Risk Analysis and HHS' Security Risk Assessment Tool). This may entail establishing an inventory of information, systems, and devices

- Document the action items identified in the risk analysis and the steps taken to address these items or establish reasonable timelines
- Verify that policies are up to date and dated, particularly pertaining to:
    - Data breach notification
    - Risk analysis and risk management
- Have supplemental documentation related to the above topics readily available and relatively self-explanatory (e.g., clearly labeled) such as:
    - Risk analyses and risk management plans
    - Documentation that addressable implementation specifications have been addressed
    - Documentation of investigations relating to breaches
    - A copy of any recent breach notifications
    - Breach risk assessments where notifications were not made
    - Documentation of the timelines from the discovery of a breach until the notifications of the breach were made
- Maintain a current list of business associates and subcontractor business associates with relevant contact information (an internal audit of accounts payable may help identify business associates and is a methodology that was used by OCR's contractors in Phase 1 audits to identify business associates)
- Confirm that appropriate workforce members have received HIPAA training (and that training has been documented)
- Prepare for an audit, perhaps including using an audit assessment tool. Consider whether it is appropriate to involve legal counsel, which may extend a privilege over the preparation process.

What to Expect from the Phase 2 Audits

For the first time, business associates will be included in OCR's HIPAA audits. OCR will request a list of business associates from covered entities (and perhaps other business associates).

Phase 2 will be conducted primarily by OCR staff. Most of these audits likely will be desk audits, although some on-site audits may occur, depending on OCR resources.

As originally announced, OCR plans to audit approximately 350 covered entities and 50 business associates. To start the audit process, OCR will verify contact information – which now is underway. Then, OCR will collect relevant information through a pre-audit

survey to select an appropriate sample. OCR will follow up with notifications and data requests to those selected for the audit.

As currently anticipated, Phase 2 audits will be more narrowly focused than the comprehensive audits in Phase 1. Phase 2 topics are to be based on deficiencies identified in Phase 1, including breach notification, risk analysis, and a corresponding risk management plan.

Covered entities and business associates will have about two weeks to respond to initial data requests. OCR has indicated that auditors will not seek clarification or additional data and only data submitted on time will be considered. OCR discourages submitting extraneous information. **OCR will not consider policies and similar documentation created after the date of the audit request.** OCR will provide a draft report to audited entities and provide an opportunity for comment prior to issuing a final report.

Projected "Round 2" of Phase 2 audits and beyond may move to device and media controls, transmission security (e.g., encryption of transmitted protected health information), Privacy Rule safeguards (e.g., governing hard copy and oral information), encryption and decryption, physical facility access controls, breach reports (e.g., to OCR), and complaint processes.

Impacts of Audits

Although OCR's communications regarding Phase 1 audits suggested that they would not be used as a vehicle for formal enforcement, OCR has indicated that Phase 2 and future audits may be more closely tied to enforcement, where adverse findings could lead to civil monetary penalties or resolution agreements.

This alert describes OCR's most recent information on its audit program. The information is subject to significant change as OCR rolls out Phase 2.

Article posted June 22, 2015 on Lexology website at:
http://www.lexology.com/library/detail.aspx?g=8ff05485-11fa-46e3-a7b7-932f024b5eb2