HDJN

The health law solution.

Phase 2 HIPAA Audits Begin: Covered Entities and Business Associates—Check Your Email!

March 22, 2016

The Office of Civil Rights (OCR) announced, yesterday, that it has commenced Phase 2 of its HIPAA Audit Program. This announcement comes in the wake of public criticism by the Office of Inspector General (OIG) regarding OCR's lack of enforcement of the Health Insurance Portability and Accountability Act (HIPAA). Phase 2 of OCR's HIPAA Audit Program will assess covered entities' and business associates' compliance with selected standards and implementation specifications of HIPAA's Privacy, Security, and Breach Notification Rules. While the Program is portrayed as a proactive compliance improvement activity that will enable OCR to identify best practices and issue technical guidance to address risks and vulnerabilities to protected health information, covered entities and business associates should be cautioned that if an audit reveals a "serious compliance issue," OCR may conduct further investigation that could lead to associated enforcement actions and potential penalties. This Phase of audits is a clear signal from OCR that business associates, not just covered entities, will be held accountable for compliance.

Background: Phase 1 Audits—Covered Entities

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") required the U.S. Department of Health & Human Services (HHS) to conduct periodic audits of covered entities and business associates to assess their compliance with the HIPAA Privacy, Security, and Breach Notification Rules. In the years 2011-2014, OCR, the branch responsible for enforcing these rules, established the HIPAA Audit Program, conducted audits of 115 covered entities, and performed extensive evaluation of the Program's protocols and effectiveness. Utilizing the knowledge obtained in Phase 1, OCR is now in a position to implement Phase 2, which will assess both covered entities and business associates.

Overview: Phase 2 Audits—Covered Entities and Business Associates

In its 2016 Phase 2 HIPAA Audit Program, OCR states that it will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules in a three phase approach. The first set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. All desk audits are scheduled to be completed by the end of 2016. The third set of audits will be onsite and will examine a broader scope of requirements than the desk audits. While the majority of the audits will be desk reviews, some desk auditees may be subject to a subsequent onsite audit. According to OCR, lessons learned in Phase 2 will be used to develop the permanent Audit Program.

What to Expect in Phase 2

The following outlines the Phase 2 notification, selection and audit process:

1. Communications from OCR are being sent via email to verify entity's address and contact information. Those who receive these communications will have fourteen (14) days to respond. Covered entities should be on the look-out for this communication and should monitor their spam email folders accordingly.
2. All covered entities (including various types of healthcare providers, health plans, and clearinghouses) and business associates are eligible for audit and will be included in the selection pool regardless of whether they respond.

For more information, Contact :

Bill Hall
bhall@hdjn.com

Mark Watson
mwatson@hdjn.com

Michelle Calloway
mcalloway@hdjn.com

3. If identified as a potential auditee, OCR will transmit a pre-audit questionnaire to gather data about size, type, and operations. As part of this pre-audit screening, OCR will be asking covered entities to identify their business associates.
4. OCR will then select a random sample of entities included in the potential audit pool for audit. Entities selected for an audit will be sent email notification of their selection and will be asked to submit documents and other data in response to a document request letter.
5. Entities notified of their participation in the audits will have ten (10) business days to upload the information requested via OCR's secure online audit portal.
6. Auditors will review the submitted documentation and develop and share draft findings with the entity.
7. Upon receipt of OCR's draft findings, auditees will have ten (10) business days to review and return written comments to the auditor. Written responses will be included in the final audit report.
8. Auditors will complete a final audit report within thirty (30) business days after the auditee's response and share a copy with the audited entity.
9. If selected for an onsite audit, entities will be notified by email of their selection. Auditors will schedule an entrance conference and provide information about the onsite audit process. Onsite audits will last three (3) to five (5) days. Drafting and finalization of OCR's report will follow the same process and timeline established for desk audits.

How to Prepare for Phase 2

It is no secret that healthcare providers' compliance programs must be proactive, not reactive, and that privacy and security of protected health information should be key components of every healthcare organization's compliance program. In accordance with these principles, a robust and effective compliance program will incorporate the following proactive measures:

1. Raise awareness within your organization to ensure that any communications from OCR are filtered to the appropriate contact so that they can be addressed promptly.
2. Continue to educate your staff on HIPAA compliance and appropriate operating procedures.
3. Ensure that privacy and security is a key component of your compliance program.
4. Review and assess your policies and procedures to ensure compliance with the standards and implementation specifications of HIPAA's Privacy, Security, and Breach Notification Rules.
5. Conduct internal self audits as part of your compliance activities. OCR plans to post updated audit protocols prior to conducting the 2016 audits that can be used to perform self-assessments.
6. Based on your self-assessments, take corrective measures to improve compliance.

While these measures are focused on covered entities' compliance programs, they are equally applicable to business associates.

If you have any questions regarding compliance with the Privacy, Security and Breach Notification rules, require assistance updating your policies and procedures, would like an independent assessment of your privacy and security compliance, or need assistance in responding to any inquiries from OCR, please contact a member of HDJN's HIPAA/Privacy & Security Team.