HINSHAW

Alerts

HHS Implements HIPAA Phase II Audit Program: What You Need to Know

March 28, 2016
Health Law Alert

Recently, the Health and Human Services Office of Civil Rights announced that it has implemented its HIPAA Phase II Audit Program. Some entities may have already received initial emails from the Office of Civil Rights (OCR) seeking audit contact information.

Which entities will be audited?

Under the Phase II Program, every covered entity and business associate is eligible for an audit. However, OCR has indicated that it is identifying pools of covered entities and business associates that represent a wide range of health care providers, health plans, health care clearing houses and business associates. The OCR believes that by auditing a broad spectrum of organizations, OCR can better assess HIPAA compliance across the industry and across the country.

What will the audits consist of?

OCR plans to primarily conduct desk audits, with some onsite audits for both covered entities and business associates. The first set of audits will be desk audits of covered entities, followed by a second round of desk audits of business associates. The desk audits will examine compliance with specific requirements of the Privacy and Security Rules, as well as breach notification requirements. Desk audits in Phase II will be completed by the end of December 2016, according to the OCR's website. The third set of audits will be onsite and will examine a broader spectrum of requirements than those under the desk audits, although some desk auditees also may be subject to an onsite audit.

What does the desk audit process entail?

The process will be the same for covered entities and business associates and will be generally as follows.

1. It starts with OCR obtaining contact information through a questionnaire designed to gather data about the size, type and operations of potential auditees. As part of that pre-audit screening questionnaire, those who OCR has selected will be asked to identify their business associates. Consequently, it would behoove covered entities to develop a list of the business associates, with contact information, so that if they are audited they will be able to respond to that request.

Attorneys

Roy M. Bossen

2. Those selected for an audit will be sent an email notification and will be asked to provide documents and other data in response to a document request letter. Audited entities will be required to submit documents online through a new secure audit portal on the OCR's website.
3. Auditors will review documentation and develop and share draft findings with the entity that has been audited.
4. Auditees will have ten business days to review and return written comments, if any, to the auditor.
5. The auditor then will complete a final report for each entity within thirty business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

What does the on-site audit process entail?

While there will be far fewer on-site audits, the on-site audits will require more personal and time resources to respond. OCR has indicated that each on-site audit will be conducted over a three to five day period, depending on the size of the institution. These audits will be more comprehensive than desk audits, and cover a wider range of requirements from the HIPAA rules. Consistent with the desk audit process, however, entities will have ten business days to review the draft findings and provide written comments. The auditors will then complete a final report for each entity within thirty business days after the auditor's response. Again, OCR will share a copy of its final report with the audited entity.

What will the findings of the audits be used for?

Generally, OCR will use the audit reports to determine types of technical assistance that should be developed, and what types of corrective action would be most helpful. However, if an audit indicates serious compliance issues, OCR may initiate a compliance review to further investigate. OCR, however, will not post a listing of audited entities, or their findings of an individual audit, which clearly identifies the audited entity, although, it is possible under the Freedom of Information Act, OCR may be required to release such information.

What should my organization be doing right now?

Both covered entities and business associates should take the time to review their policies and procedures to ensure, to the best of their ability, that they are not only up to date with required regulations, but that the practices of the entity correspond to the updated policies and procedures. Also, as mentioned earlier, covered entities should develop a list of business associates with contact information.

For further information, you may contact Roy Bossen or your regular Hinshaw attorney.