Be Prepared: Phase 2 HIPAA Audits Set to Begin

SUMMARY
On March 21, 2016, the U.S. Department of Health and Human Services, Office for Civil Rights (“OCR”), announced the launch of the 2016 Phase 2 Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Audit Program (“2016 HIPAA Audit Program”). The 2016 HIPAA Audit Program will review the policies, procedures and other activities of covered entities and business associates for compliance with the HIPAA Privacy, Security and Breach Notification Rules.

According to OCR, there will be three phases to the 2016 HIPAA Audit Program. The first phase will be desk audits of covered entities. The second phase will be desk audits of business associates. The two desk audit phases are scheduled to be completed by December 2016. The third phase will be on-site audits. The on-site audits, according to the HIPAA Audit Program website, will “examine a broader scope of requirements from the HIPAA Rules than desk audits.” Desk auditees may be subject to a subsequent on-site audit, though an entity may be selected for an on-site audit who was not the subject of a desk audit. The OCR did not provide a timeline as to when the on-site audits would be completed.

Every covered entity and business associate is eligible to be reviewed as part of the 2016 HIPAA Audit Program. According to the HIPAA Audit Program website, OCR plans to identify pools of covered entities and business associates “that represent a wide range of health care providers, health plans, health care clearinghouses and business associates.” OCR intends to select a random sample of entities in the audit pools for audit. OCR did not quantify the number of audits that will be conducted.

In order to create the audit pools, OCR will send an email to covered entities and business associates requesting that they verify their contact information. Thereafter, OCR will send a follow-up communication with a pre-audit questionnaire. According to OCR’s press release announcing the 2016 HIPAA Audit Program, an entity is still eligible for audit even if the covered entity or business associate does not verify its contact information or answer the pre-audit questionnaire. OCR will use publically available information about entities that do not respond to create its audit pool.

If selected for an audit, OCR will notify the covered entity or business associate in writing and explain the process and OCR’s expectations. For desk audits, covered entities and business associates will have 10 business days to submit the information requested by OCR to OCR through a secure on-line portal. On-site audits will be conducted over a period of three to five days. Whether a desk or on-site audit is conducted, OCR will provide the auditee with draft findings. The auditee will then have 10 business days to submit any written comments to OCR. OCR will complete an audit report within 30 business days of receiving the auditee’s response.
According to OCR, the audits are “primarily a compliance improvement activity” that are designed to give OCR a better understanding of certain HIPAA compliance efforts and to assist OCR in developing a permanent HIPAA audit program. OCR warns, however, if an audit report indicates a “serious compliance issue,” OCR may initiate a compliance review to further investigate.

While OCR states that it will not publically post a list of audited entities or the findings from an audit that individually identify an auditee, OCR may have to release this information pursuant to a Freedom of Information Act (“FOIA”) request.

The website for OCR’s HIPAA Audit Program is available at http://tinyurl.com/jpyrorz.

The 2016 HIPAA Audit Program serves as a reminder to covered entities and business associates about the need for maintaining a current and comprehensive HIPAA compliance program. If a covered entity or business associate has not recently reviewed its HIPAA compliance program, now is the time. It can be anticipated that OCR’s HIPAA compliance monitoring and enforcement activities will continue in the future.

Saul Ewing attorneys have extensive experience assisting covered entities and business associates with HIPAA compliance. Saul Ewing attorneys regularly review and create HIPAA Privacy Rule, Security Rule and Breach Notification Rule policies and procedures, train workforce members on HIPAA compliance, draft and negotiate business associate agreements, advise on HIPAA breach response and notification and assist with risk assessments. For more information on these matters, please contact the authors or the attorney at the firm with whom you are regularly in contact.

This Alert was written by Bruce D. Armon, Chair of the firm’s Health Care Practice and Managing Partner of the Philadelphia office, Karlynn Bayus, Vice Chair of the firm’s Health Care Practice, and Brenna D. Kelly, a member of the firm’s Health Care Practice. Bruce can be reached at 215.972.7985 or barmon@saul.com. Karlynn can be reached at 215.972.1892 or kbayus@saul.com. Brenna can be reached at 215.972.7874 or bkelly@saul.com.

This publication has been prepared by the Health Care Practice for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute “Attorney Advertising.”

© 2016 Saul Ewing LLP, a Delaware Limited Liability Partnership. ALL RIGHTS RESERVED.