GROOM LAW GROUP CHARTERED

BENEFITS BRIEF

April 18, 2016 www.groom.com

If you have questions, please contact your regular Groom attorney or one of the attorneys listed below:

Sravya Boppana
sboppana@groom.com
(202) 861-6338

Christy A. Tinnes
ctinnes@groom.com
(202) 861-6603

Vivian Hunter Turner
vturner@groom.com
(202) 861-6324

HHS Announces Phase II HIPAA Privacy & Security Audits

The Department of Health and Human Services (HHS) recently announced a new initiative to audit covered entities, including health plans, and their business associates for compliance with the HIPAA privacy and security rules. The HHS Office of Civil Rights (OCR) has begun to obtain and verify contact information that it will use to identify covered entities and business associates that will be audited. OCR also has issued a 420-page "Audit Protocol" that goes into detail about the types of questions that may be asked or documents that may be requested. The Audit Protocol is broken out into three "audit types": (1) HIPAA Privacy, (2) HIPAA Security, and (3) Security Breaches.

Below is a high level summary of the details we know so far about the audit process, including the information about selection of candidates, the audit timeline, and anticipated next steps in the event of audit findings.

Audit Scope

- The audit will not look at state-specific privacy and security rules.
- The HHS audit will cover the HIPAA Privacy Rule and the Security Rule.
- HHS released an "Audit Protocol" that outlines the inquiries that can be expected in an audit and the documents that would be requested. It also identifies sample documents that may be requested (e.g., request for a person to be recognized as a personal representative, whistleblower disclosures, etc.).

Audit process

- OCR has begun to obtain and verify contact information to identify covered entities and business associates of various types and determine which are appropriate to be included in potential auditee pools. See, http://www.hhs.gov/sites/default/files/ocr-address-verification-email.pdf. If an entity receives this letter it means that they may be included in the pool of potential audit candidates. It does not mean that they are being audited.
- Once entity contact information is obtained, a questionnaire designed to gather data about the size, type, and operations of potential auditees will be sent to covered entities and business associates. This data will be used with other information to develop pools of potential auditees for the purpose of making audit subject selections.
- OCR will be asking covered entity auditees to identify their business associates. We encourage covered entities to prepare a list of each business associate with contact information so that they are able to respond to this request.
- If a covered entity or business associate fails to respond to information requests, OCR will use publically available information about the entity to create its audit pool. An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

- If an entity does not respond to requests for information from OCR, including address verification, the pre-screening audit questionnaire and the document request of those selected entities, OCR will use publically available information about the entity to create its audit pool. An entity that does not respond to OCR may still be selected for an audit or subject to a compliance review.

Selection of Candidates

- Sampling criteria for auditee selection will include the size of the entity, affiliation with other healthcare organizations, the type of entity and its relationship to individuals, whether an organization is public or private, geographic factors, and present enforcement activity with OCR.
- OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review.

Three Phase Audit Program

- Desk Audits - The first set of audits will be desk audits of covered entities followed by a second round of desk audits of business associates. These audits will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules and auditees will be notified of the subject(s) of their audit in a document request letter. All desk audits in this phase will be completed by the end of December 2016.
- Onsite Audit - The third set of audits will be onsite and will examine a broader scope of requirements from the HIPAA Rules than desk audits. Some desk auditees may be subject to a subsequent onsite audit.

Audit Process

- Entities selected for an audit will be sent an email notification of their selection and will be asked to provide documents and other data in response to a document request letter.
- Audited entities will submit documents on-line via a new secure audit portal on OCR's website. There will be fewer in person visits during these Phase Two audits than in Phase One, but auditees should be prepared for a site visit when OCR deems it appropriate.
- Auditors will review documentation and then develop and share draft findings with the entity. Auditees will have the opportunity to respond to these draft findings and their written responses will be included in the final audit report.
- Audit reports will generally describe how the audit was conducted, discuss any findings, and contain entity responses to the draft findings.

Audit Timeline

- In the coming months, OCR will notify the selected covered entities in writing through email about their selection for a desk audit.
- The OCR notification letter will introduce the audit team, explain the audit process and discuss OCR's expectations in more detail. In addition, the letter will include initial requests for documentation.
- OCR expects covered entities that are the subject of an audit to submit requested information via OCR's secure portal within 10 business days of the date on the information request. All documents are to be in digital form and submitted electronically via the secure online portal.
- After these documents are received, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

Audit Findings

- Should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to further investigate. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity. However, under the Freedom of Information Act (FOIA), OCR may be required to release audit notification letters and other information about these audits upon request by the public. In the event OCR receives such a request, we will abide by the FOIA regulations.