ALSTON&BIRD

WWW.ALSTON.COM

Employee Benefits & Executive Compensation ADVISORY ■

APRIL 8, 2016

So You Heard About HIPAA Phase 2 Audits. What Should You Do Now?

by John Hickman and Steven Mindy

As you may have recently read (for example, "HHS/OCR Announces Launch of HIPAA Audit Program Phase 2"), the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) has started "Phase 2" of its audit program. Like the Phase 1 audits, OCR intends to use the audits to examine compliance mechanisms, identify best practices and discover risks and vulnerabilities to enhance compliance with HIPAA's Privacy, Security, and Breach Notification Rules. Phase 2 will be primarily desk audits, although OCR will conduct some on-site audits. If an audit reveals serious compliance issues, OCR might also launch an investigation. So now is the time to look at HIPAA compliance for your health plan and take corrective action, if needed. Business associates should do the same, as they are also subject to Phase 2 audits.

OCR's First Step – A contact letter followed by a pre-audit questionnaire

OCR's first step in the process was to email notice to verify contact information. After OCR verifies the plans' contact information, it will email a pre-audit questionnaire to gather data about the size, type and operations of potential auditees. OCR very recently posted a sample pre-audit questionnaire to its website.[1] Note that receipt of a contact letter does not mean that you will be audited. HHS says it will select a random sample, which includes not only health plans, but also health care providers and health care clearinghouses, as well as business associates.

Practice Pointer: OCR will request a list of your business associates and their contact information with the pre-audit questionnaire. If you received a contact letter, you should prepare and update your list of business associates immediately using OCR's sample template.[2]

---

1 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html

2 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html

Practice Pointer: Note that ignoring HHS's request will not exempt you from audit. HHS has said that even those that do not respond might be audited. Logically, we would not be surprised if HHS is more likely to take enforcement actions against those that do not respond. It's a good idea for those that received email notices from OCR to respond in a timely manner (and those that had the notice stuck in their "spam box" or who set the letter aside thinking they could avoid audit should reconsider responding). However, please see our note below regarding possible phishing attempts.

OCR's Second Step – Selection of auditees followed by a request to electronically submit documentation within 10 days

If selected for audit, OCR will require electronic submission of all responses within 10 business days via its secure online portal. Note that OCR plans to complete most desk audits by December 2016, so you should not wait to see if you have been selected for audit. These audits will move very quickly. In some cases, you might need to scan paper documents, such as business associate agreements, for signatures. If you receive a contact letter, you should gather your HIPAA compliance documents now and, if necessary, scan copies that are on paper only (see below for the documents OCR is expected to request).

OCR's Third Step – Desk audits

As noted, OCR will conduct some desk audits of covered entities and business associates. These audits will not necessarily be completed by December 2016, but those selected for desk audits must still submit their documents electronically.

What Documents Is OCR Expected to Request?

As of the time of publication, it does not appear that all of OCR's webpages have been updated to include links to the Phase 2 audit protocol. However, the new Phase 2 audit protocol can be found here.[3] Until very recently, OCR representatives were circulating a link regarding the Phase 1 audits as a point of reference.[4]

Auditors will not necessarily request information regarding each aspect of the Phase 2 audit protocol. However, based on informal comments from OCR representatives regarding recurring compliance issues, we expect them to request the following documents frequently:

- HIPAA Privacy Policy and Procedure.
- HIPAA Security Policy and Procedure (if separate from the Privacy Policy).
- HIPAA Breach Notification Policy and Procedure (if separate from the Privacy Policy and/or Security Policy).
- Business associate agreements, which might need to be scanned for signatures. For health plans and other covered entities, this means business associate agreements with the health plans' vendors. For entities that are business associates, this means business associate agreements with covered entities, as well as similar agreements with vendors, subcontractors or agents that handle protected health information (PHI).

---

3 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html

4 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/pilot-program/index.html

- HIPAA Risk Assessment, including evidence of security measures to reduce the risks identified in the risk analysis (e.g., risk management plan and accompanying evidence). Although tailored for health providers rather than plans, HHS's self-assessment tool[5] is a helpful guide. We expect OCR to focus heavily on:
  - Whether and how "addressable" provisions of the Security Rule were treated. "Addressable" means that the covered entity or business associate must determine whether and how to implement the rule based on the circumstances.
  - Efforts to mitigate identified risks. In particular:
    - Policies/procedures for encryption (which is "addressable" under the Security Rule), including:
      - Description of all encryption methods used.
      - Dates encryption has been in place.
      - Methods of encrypting electronic transmissions (including email).
      - Methods of encrypting mobile devices and media containing electronic PHI, and in particular, laptops and USB/thumb drives.
      - If encryption is recent, a description of alternative measures in place before encryption.
      - If a decision was made to not encrypt any particular communications or systems that contain PHI, the reason(s) for that decision.
    - Timely patching of software and updates to antivirus software.
    - Attempts to mitigate insider threats (e.g., establishment and termination of users' access to systems storing PHI, password policies, workstation access, time-out due to inactivity).
    - Procedures for disposal of PHI (both electronic and paper).
    - Data backup and contingency plans.
    - Server configurations, including descriptions of network perimeter devices like firewalls and routers.
    - Records of repair and maintenance of information systems hardware and physical security (e.g., doors and locks) in locations that contain PHI or systems containing PHI.
- Logs of unauthorized uses and disclosures of PHI, including known unauthorized uses and disclosures by business associates.
- Documents that describe investigation of potential HIPAA breaches, as well as attempts to mitigate potential and confirmed breaches.
- Breach notification letters for confirmed breaches, as well as any assessments that determined an exception applied under the breach notification requirements.
- Documentation of requests for access to, and amendment of, PHI, as well as the response to the individual.
- HIPAA notice of privacy practices, including records demonstrating timely and correct distribution, as well as links to any websites where these notices are posted.

---

5 https://www.healthit.gov/providers-professionals/security-risk-assessment

- Records demonstrating that employees with access to HIPAA PHI regularly receive HIPAA privacy and security training (e.g., attendance sheets, signed certifications), as well as applicable training materials. OCR has indicated that it favors annual HIPAA privacy and security training.
- Sanctions imposed on employees who violated HIPAA.

Note that some employers might be covered entities or business associates themselves, and their health plans might be separate covered entities. For example, a health insurance company would be a covered entity for its insured groups, a business associate for its third-party administration services and the health plan it provides its employees would be a separate HIPAA covered entity. You should be prepared to provide separate sets of documents for all covered entities and business associates that you operate.

Practice Pointer: To the extent you do not have all of these documents or have not fulfilled all the requirements, you should not lose hope. As noted, not all covered entities that receive contact letters and pre-audit questionnaires will be audited. Moreover, OCR's intent is to "use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful." Being able to show that you are taking steps to correct deficiencies might mitigate against additional HHS enforcement activities beyond correction, such as civil monetary penalties.

The Irony – watch out for phishing attempts by hackers posing as OCR to get contact information or more!

No system is perfect, and ultimately it is impossible to prevent fraud completely. That said, OCR has specifically advised covered entities and business associates to check their spam folders to ensure that all emails are received. Ironically, electronic contact letters and desk audits create an opportunity for phishing attacks by hackers who might try to obtain access to sensitive documents by sending similar emails with fake contact letters and creating their own sites for information uploads. In fairness to HHS and OCR, this could also be accomplished through the use of fake paper correspondence. Employers should ensure that their employees refer all electronic or paper inquiries that appear to be from HHS and/or OCR to a single person (for example, the privacy officer). Regardless, employers should advise employees to be on the lookout for phishing attempts related to OCR's Phase 2 audit.

Final Thoughts

If you received a notice from OCR, you should update your list of business associates and their contact information now, as you must submit this list when you receive the pre-audit questionnaire. Although OCR ultimately might not select you for audit, you should also start putting together your HIPAA documentation because the process will move very quickly for those OCR selects and all documents must be submitted electronically. Even if OCR has not notified you or does not select you for audit ultimately, an ounce of prevention goes a long way. OCR will likely conduct more audits after these Phase 2 audits, and its enforcement activities continue unabated. Conducting a self-audit and updating your HIPAA risk assessment to ensure that the appropriate procedures and documents are in place can mitigate your risk and exposure substantially.

If you would like to receive future *Employee Benefits & Executive Compensation Advisories* electronically, please forward your contact information to **employeebenefits.advisory@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Members of Alston & Bird's Employee Benefits & Executive Compensation Group

Robert A. Bauman
202.239.3366
bob.bauman@alston.com

Saul Ben-Meyer
212.210.9545
saul.ben-meyer@alston.com

Stacy C. Clark
404.881.7897
stacy.clark@alston.com

Emily Seymour Costin
202.239.3695
emily.costin@alston.com

Patrick C. DiCarlo
404.881.4512
pat.dicarlo@alston.com

Meredith Gage
404.881.7953
meredith.gage@alston.com

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

David R. Godofsky
202.239.3392
david.godofsky@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

H. Douglas Hinson
404.881.7590
doug.hinson@alston.com

Emily C. Hootkins
404.881.4601
emily.hootkins@alston.com

James S. Hutchinson
212.210.9552
jamie.hutchinson@alston.com

Jahnisa Tate Loadholt
202.239.3670
jahnisa.loadholt@alston.com

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

Steven Mindy
202.239.3816
steven.mindy@alston.com

Craig R. Pett
404.881.7469
craig.pett@alston.com

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Jonathan G. Rose
202.239.3693
jonathan.rose@alston.com

Syed Fahad Saghir
202.239.3220
fahad.saghir@alston.com

Thomas G. Schendt
202.239.3330
thomas.schendt@alston.com

John B. Shannon
404.881.7466
john.shannon@alston.com

Richard S. Siegel
202.239.3696
richard.siegel@alston.com

Leah Singleton
404.881.7568
leah.singleton@alston.com

Carolyn E. Smith
202.239.3566
carolyn.smith@alston.com

Michael L. Stevens
404.881.7970
mike.stevens@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Elizabeth Vaughan
404.881.4965
beth.vaughan@alston.com

Kerry T. Wenzel
404.881.4983
kerry.wenzel@alston.com

Kyle R. Woods
404.881.7525
kyle.woods@alston.com

ALSTON&BIRD

WWW.ALSTON.COM