ALSTON&BIRD

WWW.ALSTON.COM

Employee Benefits & Executive Compensation ADVISORY ■

AUGUST 23, 2016

HIPAA Phase 2 Audits: What Has OCR Requested from Auditees to Date?

by John Hickman and Steven Mindy

In our April 8, 2016, advisory, we discussed the U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR) "Phase 2" audit program. Then, we could only make educated guesses about what documents OCR would likely request from auditees. However, on July 11, 2016, OCR contacted the covered entities it selected. Although the tight 10-day turnaround caused some angst for those audited, the scope of OCR's requests (drawn directly from the OCR audit protocol document) was less onerous than many predicted (especially given the length of the protocol document).

That said, while HIPAA-covered entities that were not selected can breathe a deep sigh of relief (for now), the audit activity is far from over. As part of its Phase 2 audit program, OCR will next audit business associates based on the information the covered entities provide. Additionally, OCR will conduct onsite audits of covered entities and business associates. It is unclear whether this may include covered entities and business associates that OCR did not select for original desk audits, as OCR said, "*[s]ome* desk auditees may be subject to a subsequent onsite audit." Moreover, on August 18, 2016, OCR announced an immediate initiative by its regional offices to increase the number of investigations of breaches that affect fewer than 500 individuals.

Phase 2 Documents Requested: List of Business Associates Via E-mail

Unsurprisingly, OCR requested a list of business associates. OCR provided the following sample template to help auditees respond:

BA Name	Type of Service Provided	POC1 Title	POC1 First Name	POC1 Last Name	POC1 Address	POC1 Address Continued	POC1 City
UNITED COUNSELING SERVICE OF BENNINGTON COUNTY, INC.		HR Director	Amy	Fela	PO BOX 588		BENNINGTON
Asociacion De Maestros De Puerto Rico		President	Aida	Diaz de Rodriguez	452 Ponce de León Ave		San Juan
Idaho Department of Health & Welfare		Privacy Officer	Heidi	Graham	PO Box 83720		Boise
NEXUS LAB, INC.		Interm Compliance Officer	Anna	Whitef	PO Box 1240		RUSSELL SPRINGS
ANTONIO ESPARZA, M.D., P.A.		Office Manager	Irene	Paramo	900 W SAM HOUSTON	SUITE1	PHARR

Notably, OCR only requested documents from HIPAA-covered entities during this first stage of the Phase 2 audits. During the next stage, OCR will select business associates for audit from the lists covered entities provided.

Phase 2 Documents Requested: Privacy Rule & Breach Notification Rule Documents or Security Rule Documents Via Secure Website Upload

Although OCR required auditees to submit their list of business associates by e-mail, it provided a secure website for auditees to upload the other documents they requested. In a webinar, OCR indicated that "entities will either be audited on [Security Rule] controls or [Privacy Rule & Breach Notification Rule] compliance."

The documents that OCR typically requested of covered entities selected for Privacy Rule and Breach Notification Rule audits included:

- All HIPAA notices of privacy practices posted on the entity's website, within its facility or distributed to individuals that were in place at the end of 2015. In its desk audit guidance, OCR clarified that this includes translations.
- The URL for the website where the notice of privacy practices was posted, if any. In addition, if electronic notice was provided, OCR requested its policies and procedures regarding electronic distribution, as well as a sample of an individual's consent to receive the notice via e-mail or electronically.
- Policies and procedures for individuals to request access to protected health information (PHI), as well as the documentation for the first access requests granted, and evidence fulfillment in 2015. OCR also requested documentation for the last five access requests that the entity extended its time for response, as well as any standard template or letter that the entity uses or requires to grant access requests. When a third-party administrator decides access requests for a health plan, HHS stated in a Q&A that the covered entity should provide a description of how the business associate handles access requests in the comment section. Thankfully, the desk audit guidance clarified that access requests do not include third-party disclosure requests that are merely authorized by an individual.
- Documentation for five breach incidents in 2015 involving fewer than 500 individuals, including the date individuals were notified, the date the covered entity discovered the breach and the reasons for any delayed notification.
- Documentation for five breach incidents involving 500 or more individuals in 2015, including one written notice sent to an affected individual for each breach, and any standard templates or form letters.

OCR desk audits for the Security Rule can include:

- HIPAA risk analysis policies and procedures for the six years before the audit request date. OCR also required entities to provide documents from 2015 showing that these documents were available to the individuals responsible for implementing the policies and procedures and that they were reviewed periodically and updated as needed.
- The most recent HIPAA risk analysis, the risk analysis immediately before it and the results. In the Q&A, HHS stated that it did not want covered entities to create a new risk analysis if the risk analysis is not up to date. Also, although some entities raised concerns that disclosure of this information could become public knowledge under the Freedom of Information Act (FOIA), OCR stated in its desk audit guidance that it believes the information is exempt from the FOIA as "trade secrets or commercial or financial information

that is confidential or privileged." However, OCR noted in its webinar that it might be required to release audit notification and other information about these audits under the FOIA.

- HIPAA risk management policies and procedures regarding risk management for the six years before the audit date. OCR also required entities to provide documents from 2015 showing that these documents were available to the individuals responsible for implementing the policies and procedures and that they were reviewed periodically and updated as needed. OCR's desk audit guidance says evidence that the policies and procedures were available to responsible individuals would include screen shots that show document properties and mapped drive permissions.
- The documents showing efforts used to manage risks in 2015, as well as the measures implemented to reduce risks based on the current risk analysis.

Uploading Documents for Phase 2: Be Careful Before You Press Submit!

OCR hosted an informational webinar shortly after it notified selected covered entities. The webinar included screenshots of what auditees can expect to see when they upload their documents, such as:

Of great significance to those responsible for uploading the document, OCR noted in the Q&A during the webinar that "once an entity selects the 'review and submit' button, you cannot return to the system to delete and replace files previously uploaded."

If I'm a Covered Entity That's Also a Business Associate, Can I Also Expect to Be Audited as a Business Associate?

During its Q&A, OCR stated that "[i]t is possible, but not likely" that OCR will select them for another audit if they are the business associate of another covered entity, which might provide some comfort to covered entities that OCR selected for desk audits.

Is OCR Also Increasing the Number of Breach Investigations?

Yes. OCR currently investigates *all* breaches involving 500 or more individuals. On August 18, 2016, OCR announced an immediate initiative by its regional offices to increase investigations of breaches involving fewer than 500 individuals. Regional offices will identify and obtain corrective action to address entity and systemic noncompliance related to these breaches. Regional offices will consider, among other things:

- The size of the breach.
- Theft of or improper disposal of unencrypted PHI.
- Breaches that involve unwanted intrusions to IT systems (for example, hacking).
- The amount, nature and sensitivity of the PHI involved.

- Instances where numerous breach reports from a particular covered entity or business associate raise similar issues.

When OCR conducts investigations, it often assesses penalties for not conducting a risk assessment and/or not having adequate security policies and procedures. For example, after the theft of an unencrypted smartphone with the PHI of 412 individuals, OCR assessed a $650,000 penalty for not having security incident and mobile device policies.

Even before OCR's announcement, we noticed a marked increase in the investigation of small breaches, particularly when there was a pattern of small breaches. Covered entities and business associates must be careful because these investigations often result in substantial monetary penalties for not maintaining adequate policies, procedures and/or records of risk assessments.

Conclusion

No one is off the hook yet. Although OCR made its Phase 2 desk audit requests for covered entities, business associates are next. And covered entities and business associates remain subject to onsite audits whether or not they were selected for a desk audit. Moreover, this year's foray into the audit world is proving to be a mere prelude to more detailed investigations involving small breaches, as OCR recently just announced its new investigation initiative. It would be wise to ensure that you can provide the documents HHS has requested to date during its Phase 2 desk audits, as well as any other documents required to comply with HIPAA (including the ones mentioned in our April 8, 2016, advisory in case you are selected for a desk audit or are investigated due to a breach).

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

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

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333