



ACA, HIPAA AND  
FEDERAL HEALTH  
BENEFIT MANDATES:

# Practical Q&A

*The Affordable Care Act (ACA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other federal health benefit mandates (e.g., the Mental Health Parity Act, the Newborns and Mothers Health Protection Act, and the Women's Health and Cancer Rights Act) dramatically impact the administration of self-insured health plans. This monthly column provides practical answers to administration questions and current guidance on ACA, HIPAA and other federal benefit mandates.*

*Attorneys John R. Hickman, Ashley Gillihan, Carolyn Smith, and Dan Taylor provide the answers in this column. Mr. Hickman is partner in charge of the Health Benefits Practice with Alston & Bird, LLP, an Atlanta, New York, Los Angeles, Charlotte and Washington, D.C. law firm. Ashley Gillihan, Carolyn Smith and Dan Taylor are members of the Health Benefits Practice. Answers are provided as general guidance on the subjects covered in the question and are not provided as legal advice to the questioner's situation. Any legal issues should be reviewed by your legal counsel to apply the law to the particular facts of your situation. Readers are encouraged to send questions by E-MAIL to Mr. Hickman at [john.hickman@alston.com](mailto:john.hickman@alston.com).*

## HIPAA Phase 2 Audits:

### What has OCR requested from auditees to date?'

In our May article, 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<sup>2</sup>, OCR contacted the covered entities it selected. Although, the tight 10 day turn-around caused some angst for those audited, the scope of OCR's requests (drawn directly from the OCR audit protocol document) were less onerous than many predicted (especially given the length of the protocol document). That said, while HIPAA covered entities that were not selected can take 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 on-site 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<sup>3</sup>."

### Documents Requested: List of Business Associates via E-mail

Unsurprisingly, OCR requested a list of business associates. OCR provided the following sample template (available at <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html>) to help auditees respond:

BA Name	Type of Service Provided	POCI Title	POCI First Name	POCI Last Name	POCI Address	POCI Address Contained	POCI City
UNITED COUNSELING SERVICE OF BENNINGTON COUNTY, INC.		HR Director	Amy	Fala	PO BOX 688		BENNINGTON
Asociacion De Maestros De Puerto Rico		President	Aida	Diaz de Rodriguez	452 Ponce de Leon Ave		San Juan
Idaho Department of Health & Welfare		Privacy Officer	Miguel	Graham	PO Box 83720		Boise
NEKUS LAB, INC.		Interim Compliance Officer	Jennie	White	PO Box 1240		RUSSELL SPRINGS
ANTONIO ESPARZA, M.D., P.A.		Office Manager	Irene	Paramo	100 W SAM HOUSTON, SUITE 1		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.

### 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<sup>4</sup>, OCR indicated that "entities will either be audited on [Security Rule] controls or [Privacy Rule & Breach Notification Rule] compliance." The documents<sup>5</sup> that OCR typically requested of covered entities selected for Privacy Rule and Breach Notification Rule audits included:

**1** 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<sup>6</sup>, OCR clarified that this includes translations.

**2** 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.

**3** Policies and procedures for individuals to request access to 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<sup>7</sup> 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.

**Experience You Can Trust**  
**Results You Want**  
**Service You Expect!**



**EthiCare Advisors** has saved millions of dollars for our clients since our inception in 2002. While our proven cost saving solutions for high-dollar and dialysis claims continue to make us a market leader, we also offer new services that have been developed in conjunction with our clients, including HIPAA Compliance Solutions, Forensic Cost Containment and Expert Witness Services. **Contact us today to leverage our experience for generating the results you want with the service you expect.**



**Contact Us Today**  
**info@EthiCareAdvisors.com**  
**888.838.4422**

**4** Documentation for five breach incidents in 2015 involving less than 500 individuals, including the date individuals were notified, the date the covered entity discovered the breach, and the reasons for any delayed notification.

**5** 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:**

**1** HIPAA risk analysis policies and procedures for the six (6) 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.

**2** 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 FOIA, OCR stated in its desk audit guidance that it believes the information is exempt from FOIA as “trade secrets or commercial

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

**3** HIPAA risk management policies and procedures regarding risk management for the six (6) 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.

**4** 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: be careful before you press submit!**

OCR hosted an informational webinar<sup>8</sup> shortly after it notified selected covered entities. The webinar included screenshots of what auditees can expect to see when the 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.

## Conclusion

No one is off the hook, yet. Although OCR made its Phase 2 desk audit requests for covered entities, business associates are next. Moreover, covered entities and business associates may remain subject to on-site audits regardless of whether or not they were selected for a desk audit. We can also expect that this year's foray into the audit world will prove to be a mere prelude to more detailed investigations in years to come. Thus, 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 May article in case you are selected for a desk audit). ■

## References

<sup>1</sup> Steven Mindy, an associate in Alston & Bird's Washington DC office co-authored this article.

<sup>2</sup> <http://www.hhs.gov/hipaafor-professionals/compliance-enforcement/audit/index.html#responsible>

<sup>3</sup> <http://www.hhs.gov/hipaafor-professionals/compliance-enforcement/audit/>

<sup>4</sup> Webinar available at <http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf>

<sup>5</sup> <http://www.hhs.gov/hipaafor-professionals/compliance-enforcement/audit/index.html#responsible>

<sup>6</sup> <http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf>

<sup>7</sup> Q&A available at <http://www.hhs.gov/sites/default/files/Phase2AuditOpeningMeetingWebinarQ%26A.pdf>

<sup>8</sup> Webinar available at <http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf>

