Phase 2 HIPAA Audits Underway: What Covered Entities and Business Associates Need to Know

H. Carol Saul and Madison M. Pool

On March 21, 2016, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced the beginning of Phase 2 of its HIPAA audits of covered entities and their business associates.[1] Per the OCR announcement, "OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted."[2] Although OCR has announced that only a few hundred covered entities and business associates will be audited during Phase 2,[3] OCR has not disclosed exact numbers and has been specific that every covered entity and business associate is eligible for an audit.[4] In addition, OCR has said that it will use the results of the Phase 2 Audits to develop its permanent audit program,[5] underscoring that this increased audit activity is likely to continue into the future.

History of the Audit Program

The Health Information Technology for Economic and Clinical Health Act (HITECH) requires OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules.[6] In 2011 and 2012, OCR implemented a pilot audit program, referred to as "Phase 1", in which it audited only 115 covered entities for compliance with HIPAA's requirements.[7] Drawing on the Phase I experience and results, OCR is now implementing Phase 2 of the program.[8] Phase 2 expands the audit scope to include business associates as well as covered entities.[9] OCR will not audit entities with open complaint investigations.[10]

This increase in audit activity comes just a few months after the OIG issued two reports calling for better oversight of covered entities.[11] The first report, titled "OCR Should Strengthen its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards," found that OCR's oversight is primarily reactive and that OCR had not fully implemented the required audit program to proactively assess possible noncompliance from covered entities. OIG recommended in part that OCR fully implement a permanent audit program and develop a policy requiring OCR staff to check whether

1 Dep't of Health & Human Services Office for Civil Rights, *OCR Launches Phase 2 of HIPAA Audit Program*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html (last visited Mar. 25, 2016) [*hereinafter* Phase 2 Article].
2 Phase 2 Article.
3 David Raths, OCR's Samuels Describes Launch of Phase 2 of HIPAA Audit Program, HEALTHCARE INFORMATICS (Mar. 19, 2016), http://www.healthcare-informatics.com/article/ocr-ramping-200-hipaa-audits-2016.
4 *Dep't of Health & Human Services Office for Civil Rights, HIPAA Privacy, Security, and Breach Notification Audit Program*, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html (last visited Mar. 25, 2016) [*hereinafter* HIPAA Audit Program Article].
5 Phase 2 Article.
6 Pub. L. 111-5, § 13411 (123 STAT. 276; 42 USC 17940), Feb. 17, 2009, *available at* https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf.
7 HIPAA Audit Program Article.
8 HIPAA Audit Program Article.
9 HIPAA Audit Program Article.
10 HIPAA Audit Program Article.
11 Dep't of Health & Human Services Office of the Inspector General, *OCR Should Strengthen its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards*, OEI-09-10-00510 (Sept. 2015), *available at* http://www.oig.hhs.gov/oei/reports/oei-09-10-00510.pdf.

covered entities had previously been investigated for noncompliance.[12]

The second OIG report, "OCR Should Strengthen its Follow-up of Breaches of Patient Information Reported by Covered Entities," found that OCR had incomplete documentation of covered entities' corrective actions in 23% of closed "large-breach" cases in which OCR made determinations of noncompliance.[13] OIG also found that OCR did not record "small-breach" information in its case-tracking system, which limits its ability to track and identify covered entities with multiple small breaches.[14] OIG's recommendations included that OCR maintain complete documentation of corrective actions taken and enter small-breach information into its case-tracking system.[15]

OCR agreed with OIG's recommendations in both reports and has begun to proactively implement programs to address the issues and recommendations identified in them.

Recommendations for Covered Entities and Business Associates

Although OCR has indicated that the 2016 Phase 2 audit program is "primarily a compliance improvement activity" aimed at identifying the types of technical assistance to develop and corrective actions that would be most helpful,[16] the program is not the only reason an entity should consider putting its HIPAA house in order. HIPAA noncompliance poses financial risks to covered entities and business associates. OCR's $1.55 million settlement with North Memorial Health Care of Minnesota (North Memorial) earlier this month illustrates the serious risk of noncompliance.[17] An audit is not the only way noncompliance can come to OCR's attention—the North Memorial settlement followed a breach report by North Memorial disclosing a breach by a business associate.[18] The settlement resolved allegations that North Memorial had violated HIPAA by not implementing a business associate agreement where required and failing to conduct an organization-wide HIPAA risk analysis.[19] In addition to the payment, North Memorial is also required to develop an organization-wide risk analysis and risk management plan, as well as to train appropriate workforce members on all policies and procedures newly developed or revised pursuant to the corrective action plan.[20]

Covered entities and business associates should be aware of the increased scrutiny and heightened enforcement of HIPAA compliance. Some general recommendations to consider are:

1. **Be alert for e-mails from OCR.** The first step of the 2016 audit process will be an e-mail from OCR requesting verification of an entity's address and contact information.[21] Receipt of an e-mail does not necessarily mean that an entity has been selected for audit, but not responding to a request for information will not exempt an entity from the audit pool.[22] In other words, an entity that does not respond may still be selected for audit, and OCR has expressed an expectation that entities will provide full cooperation and support, even expressly stating that OCR expects covered entities and business associates to check junk or spam email folders for emails from OCR, (OSOCRAudit@hhs.gov), in anticipation of the requests for information.[23] Note also, that if an entity receives a request for information and does not respond, OCR will use publicly available information to create its audit pool,

12 Dep't of Health & Human Services Office of the Inspector General, OCR Should Strengthen its *Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards*, OEI-09-10-00510 (Sept. 2015), *available at* http://www.oig.hhs.gov/oei/reports/oei-09-10-00510.pdf.
13 Dep't of Health & Human Services Office of the Inspector General, OCR Should Strengthen its Follow-up of Breaches of Patient Information Reported by Covered Entities, OEI-09-10-00511 (Sept. 2015), *available at* http://oig.hhs.gov/oei/reports/oei-09-10-00511.pdf.
14 Dep't of Health & Human Services Office of the Inspector General, OCR Should Strengthen its Follow-up of Breaches of Patient Information Reported by Covered Entities, OEI-09-10-00511 (Sept. 2015), *available at* http://oig.hhs.gov/oei/reports/oei-09-10-00511.pdf.
15 Dep't of Health & Human Services Office of the Inspector General, OCR Should Strengthen its Follow-up of Breaches of Patient Information Reported by Covered Entities, OEI-09-10-00511 (Sept. 2015), available at http://oig.hhs.gov/oei/reports/oei-09-10-00511.pdf.
16 HIPAA Audit Program Article.
17 Press Release, Dep't of Health & Human Services, $1.55 million settlement underscores the importance of executing HIPAA business associate agreements (Mar. 16, 2016), *available at* http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html [*hereinafter* Press Release].
18 Press Release.
19 Press Release.
20 Press Release (the Resolution Agreement and Corrective Action Plan can be found on the HHS website at: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/north-memorial-health-care/index.html).
21 Phase 2 Article.
22 HIPAA Audit Program Article.
23 HIPAA Audit Program Article.

potentially creating confusion and increasing the risk of missing the 10 business day response time for entities ultimately selected for an audit.[24]

2. **Evaluate HIPAA compliance.** With OCR's increased scrutiny of covered entities and business associates, organizations should proactively evaluate their HIPAA compliance programs. OCR has said that it will post updated audit protocols on its website closer to conducting the 2016 audits.[25] While the updated protocols will be the best tool for organizations to conduct their own internal self-audits as part of their HIPAA compliance activities, covered entities and business associates need not wait for the revised protocols prior to self-evaluating. The Phase 1 protocols are available here[26] and provide useful guidance for the present time.

3. **Address any compliance gaps.** If a covered entity or business associate identifies any gaps in its HIPAA compliance, it should take steps to address them. Entities should also consider whether any identified issues or updates trigger a notice requirement (for example, notice to patients of an updated Notice of Privacy Practices). We anticipate that organizations will be required to provide copies of their security risk assessment and their breach notification policy, among other items.

4. **Document, document, document.** As always, covered entities and business associates should ensure that they appropriately document their compliance efforts. Not only will this exercise help keep an entity on track with its HIPAA compliance, it will also place the entity in a better position to timely support an assertion of compliance should it receive a request for information from OCR or be selected for an audit. Note that covered entities will be asked to provide a list of all of their business associates as part of the 2016 pre-audit screening questionnaire,[27] and this and other similar requests may be challenging to meet in a short time frame if the information is not already readily available. OCR expects organizations to submit all documents and responses to an audit within 10 business days of the date the audit request is received.

24 HIPAA Audit Program Article.
25 Phase 2 Article.
26 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html
27 HIPAA Audit Program Article.

Authors and Contributors

H. Carol Saul
Partner, Atlanta Office
404.873.8694
carol.saul@agg.com

Madison M. Pool
Associate, Atlanta Office
404.873.8514
madison.pool@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**