2017 HIPAA Enforcement: Year to Date Lessons

Kevin L. Coy and Madison M. Pool

With the announcements from OCR of three resolution agreements and one civil money penalty as of mid-February, OCR is off to a record start for HIPAA enforcement in 2017, with double the announcements as the same time last year.[1] Notably, this swift initial series of HIPAA enforcement actions has been announced following—and foreshadows rivaling—what was also a record-setting year for OCR enforcement in 2016. Based on the announcements thus far this year, OCR appears to be continuing its focus on compliance with the HIPAA Security Rule and protection for electronic protected health information ("ePHI"). Covered entities and business associates alike should heed the lessons learned from these announcements and take steps to review their HIPAA compliance and bolster it as necessary.

I. 2016 Recap

2016 saw the highest number of OCR HIPAA resolution agreements of any prior year, doubling to 12 from the previous two years' six each.[2] What is perhaps even more striking is the total settlement amount for 2016: whereas the number of settlements doubled from 2015 to 2016, the dollars nearly quadrupled. The $23.5 million assessed in 2016 resolution agreements and civil money penalties was almost four times the $6.19 million of 2015.[3] Considering the size of the penalties assessed thus far in 2017, coupled with the approximately 10% increase in penalty amounts in September 2016 (which were effective for penalties assessed after August 1, 2016, including penalties whose associated violations occurred after November 2, 2015)[4], it seems likely that we will see continued high-dollar settlements from OCR in 2017.

II. Resolution Agreements and Civil Money Penalties as of 2/16/2017

OCR may investigate a covered entity or business associate for any of several reasons—e.g., in response to a breach report or a complaint, or simply through a random audit—and investigations are not limited to the scope of the initial reason for OCR's investigation. However, even limiting the potential reasons for an OCR investigation only to filed breach reports affecting 500 or more individuals, the volume of potential investigatory actions is significant. There were nearly 330 such breach reports in 2016.[5] Further, OCR may resolve investigated issues in a variety of ways; some will be resolved by OCR determining there was no violation or that the violation has been satisfactorily resolved, some will be resolved through informal technical assistance and corrective action, and others will be resolved via resolution agreements or civil money penalties.[6] As these final two resolutions are the only methods publicly announced, review of the announced resolutions is valuable to covered entities and business associates for the insight they provide into areas of particular focus for OCR.

1 See HHS.gov, *Resolution Agreements*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ (last visited Feb. 20, 2017).
2 *Id.*
3 *Id.*; see also http://www.agg.com/HHS-OCR-Levies-Significant-HIPAA-Penalties-in-a-Series-of-Recent-Settlements-Covered-Entities-and-Business-Associates-Alike-Should-Review-Practices-12-15-2016/ (last visited Feb. 20, 2017).
4 45 C.F.R. Part 102; see also 45 C.F.R. 160.404.
5 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
6 HHS.gov, *Enforcement Data*, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html (last visited Feb. 20, 2017).

A. January 9, 2017 Resolution Agreement: Importance of Timely Breach Reporting

The first resolution agreement of 2017[7] announced on January 9, 2017, between HHS and Presence Health was the first ever HIPAA settlement based on the untimely reporting of a breach.[8] Although Presence did comply with the HIPAA breach reporting requirements, the belated reports were approximately 41 days past due. One notable quote from OCR's announcement of this resolution agreement reveals just how serious OCR considered this delay to be: "With this settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether." In other words, it seems that it is OCR's opinion that $475,000 was a low settlement amount—and that a higher amount would have been justified—given the delay in reporting.

B. January 18, 2017 Resolution Agreement: Importance of Implementing Risk Management Plans

The second resolution agreement of 2017 was announced on January 18, 2017, between HHS and MAPFRE Life Insurance Company of Puerto Rico.[9] The settlement amount was $2.2 million and was predicated on a 2011 breach report filed by the company following discovery that a flash drive had been stolen.[10] The breach affected 2,209 individuals and, per the press release, OCR's investigation revealed several deficiencies in the company's HIPAA security compliance, including "a failure to conduct its risk analysis and implement risk management plans, contrary to its prior representations, and a failure to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014."[11] OCR also noted that the company had "failed to implement or delayed implementing other corrective measures it informed OCR it would undertake."[12] A significant portion of OCR's analysis focuses on the lack of implementation of safeguards for ePHI, especially those the company had previously identified and indicated that it would take.

C. February 1, 2017 Civil Money Penalty: Importance of Encryption for Electronic Devices

On February 1, 2017, OCR announced the first civil money penalty of the year with Children's Medical Center of Dallas, stemming from two separate breach reports each involving the loss or theft of an unencrypted device.[13] In total, approximately 6,262 individuals were affected.[14] OCR cites a number of deficiencies in Children's HIPAA compliance, including "a failure to implement risk management plans, contrary to prior external recommendations to do so, and a failure to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April 9, 2013." Although not required by regulation, OCR made clear its expectation here that Children's should have utilized encryption on such devices, noting that "[d]espite Children's knowledge about the risk of maintaining unencrypted ePHI on its devices as far back as 2007, Children's issued unencrypted BlackBerry devices to nurses and allowed its workforce members to continue using unencrypted laptops and other mobile devices until 2013."

D. February 16, 2017 Resolution Agreement: Importance of Access Controls and Audit Log Review

On February 16, 2017, OCR announced a resolution agreement with Memorial Healthcare Systems that includes

7 http://www.agg.com/HIPAA-Breach-Notify-Promptly-or-Face-Significant-Potential-Fines-from-HHS-OCR-01-24-2017/

8 HHS, First HIPAA enforcement action for lack of timely breach notification settles for $475,000, http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html (last visited Feb. 20, 2017); see also http://www.agg.com/HIPAA-Breach-Notify-Promptly-or-Face-Significant-Potential-Fines-from-HHS-OCR-01-24-2017/

9 HHS, HIPAA settlement demonstrates importance of implementing safeguards for ePHI, http://wayback.archive-it.org/3926/20170127111936/https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html (last visited Feb. 2, 2017).

10 *Id.*

11 *Id.*

12 *Id.*

13 HHS, Lack of timely action risks security and costs money - February 1, 2017, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/childrens (last visited Feb. 20, 2917).

14 *Id.*

a settlement amount of $5.5 million - a figure that nearly matches the highest settlement ever with a single entity.[15] (We hesitate to refer to this as the "most recent settlement" because, at the rate of the announcements, there may well be another between the time this article is sent to print and is released. For the most up-to-date information on OCR settlement agreements, see HHS' webpage, "Resolution Agreements: Resolution Agreements and Civil Money Penalties, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/.)

The OCR investigation and resolution arose after Memorial reported a breach of PHI of 115,143 individuals to HHS that occurred when an unauthorized individual utilized the "login credentials of a former employee of an affiliated physician's office."[16] Per OCR, these login credentials had been used "on a daily basis without detection from April 2011 to April 2012."[17] Central to OCR's analysis was the fact that Memorial "failed to implement [its existing] procedures with respect to reviewing, modifying and/or terminating users' right of access."[18] OCR also cited Memorial's failure to "regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by [Memorial] from 2007 to 2012."

III. Practical Takeaways

Although all areas of HIPAA compliance are important and should be closely reviewed, these recent HIPAA enforcement actions give covered entities and business associates indications of where OCR is focusing its attention and, thus, suggest areas to prioritize their compliance efforts in 2017:

- **Timely Breach Assessment and Reporting:** As indicated by the Presence Health resolution agreement, OCR takes breach reporting requirements very seriously, including the deadlines for reporting. Accordingly, covered entities and business associates should act quickly upon becoming aware of a potential HIPAA breach and ensure that notice is provided as required within the designated timeframe, even if the investigation is not entirely concluded and the entity has to supplement the notice once more information is available.

- **Risk Assessment:** Many of OCR's announced resolution agreements of 2016 and thus far in 2017 have focused on the importance of conducting the required security risk assessment. OCR has made very clear that this is a high priority, and covered entities and business associates should ensure that they have conducted a thorough, compliant assessment that addresses all of the entity's ePHI, and that the assessment is updated periodically and as needed (e.g., following a merger or acquisition, or the implementation of new software, etc.).

- **Implementation of Risk Mitigation Measures:** Not only must an entity conduct a risk assessment, it must identify risk mitigation measures. Once identified, the entity should take concrete steps to implement the identified measures or risk additional or increased penalties from OCR for failing to adequately safeguard ePHI.

- **Encryption:** The only item on the list that is not expressly required by the regulations - encryption (and, more specifically, lack thereof) - has received focused attention from OCR. Covered entities and business associates should give careful consideration to implementing encryption for mobile devices, laptops, and other systems where available. If an entity determines that encryption is not feasible or reasonable, that determination should be carefully documented, and the entity should ensure that appropriate alternative protective measures have been put in place.

- **Audit Controls:** Compliance with the HIPAA Security Rule is not a one-time activity; ongoing monitoring and auditing are required. Failure to conduct such reviews is itself a potential violation of HIPAA, and failure to detect and address security incidents and breaches that could have been identified through such reviews can also lead

15 HHS, $5.5 million HIPAA settlement shines light on the importance of audit controls, https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html (last visited Feb. 20, 2017); see also HHS, Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html (last visited Feb. 20, 2017).
16 *Id.*
17 *Id.*
18 *Id.*

to separate, additional violations. Covered entities and business associates should review their policies related to audit controls, update them as necessary, and ensure that they are implemented consistently.

- **Business Associate Agreements:** Although not a focus of the 2017 enforcement actions to date, having updated business associate agreements in place, where needed, was a focus of multiple enforcement actions in 2016, and is a lesson to carry over into 2017.

Authors and Contributors

Kevin L. Coy
Partner, DC Office
202..677.4034
kevin.coy@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/**