HHS OCR Levies Significant HIPAA Penalties in a Series of Recent Settlements: Covered Entities and Business Associates Alike Should Review Practices

Kevin Coy

Between June and November 2016, the Department of Health and Human Services Office of Civil Rights (HHS OCR) has announced seven high-dollar settlements to resolve alleged violations of the HIPAA privacy, security, and breach notification rules by both covered entities and business associates. Penalties ranged from $400,000 to $5.5 million (the largest HIPAA settlement to date against a single entity). In addition to announcements that OCR intends to increase scrutiny of data breaches involving fewer than 500 individuals[1] and HHS OCR's ongoing HIPAA audit program, these settlements underscore the importance of HIPAA compliance both for covered entities and for business associates.

It is important to note that while one or more data breaches were the initial catalyst for each of these investigations, once HHS OCR initiates an inquiry, the agency does not necessarily limit its attention to the facts of that breach. HHS OCR can examine all aspects of compliance with the Privacy, Security, and Breach notification rules. The substantial penalties that can result from an HHS OCR inquiry do not necessarily turn on the size of the underlying data breach. For example, a $650,000 settlement in June resulted from an investigation prompted by a breach affecting 412 individuals.[2] Size can matter, however. The largest HIPAA settlement to date, $5.5 million, followed a breach affecting approximately 4 million individuals.[3]

The seven recent settlements, from the highest civil penalty amount to the lowest, addressed a range of alleged HIPAA violations:

- **Advocate Health Care.** In August, HHS OCR announced that Advocate Health Care agreed to pay $5.5 million after the potential compromise of PHI of approximately 4 million individuals. HHS OCR alleged that Advocate failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI; failed to implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center; failed to obtain satisfactory assurances in the form of a written business associate agreement that a business associate would appropriately safeguard all ePHI in its possession; and failed to reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.[4]

- In July, HHS OCR announced a pair of HIPAA settlements with the University of Mississippi Medical Center and Oregon Health and Science University, for $2.75 million and $2.7 million respectively.

    - **University of Mississippi.** In the case of the University of Mississippi, HHS OCR alleged, following a breach that exposed the PHI of approximately 10,000 individuals, that the University had failed to implement policies and procedures to address security violations; failed to implement physical safeguards for all workstations with access to ePHI to restrict access to authorized users; failed to

1 http://www.agg.com/HHS-Office-for-Civil-Rights-to-Increase-Investigation-of-Small-HIPAA-Breaches-08-29-2016/
2 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html
3 http://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html
4 http://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html

assign unique user IDs to track who was accessing ePHI; and failed to notify each individual reasonably believed to have been implicated in the breach.[5]

- **OHSU.** In the case of Oregon Health and Science University, HHS OCR alleged "widespread and diverse problems" after an investigation triggered by multiple breach reports involving thousands of individuals. Alleged failings included: failure to enter into a business associate agreement with a cloud service provider (HHS OCR subsequently published new guidance on this topic in October)[6]; failure to conduct comprehensive risk assessments and address issues found in those risk assessments; failure to implement appropriate policies and procedures to protect PHI; and failure to implement a mechanism to encrypt and decrypt ePHI (or employ an equivalent alternative) on its workstations.[7]

- **St. Joseph Health.** In October, HHS OCR announced that St. Joseph Health agreed to pay $2.14 million after the PHI of 31,800 patients was potentially exposed because a server included a file sharing application with default settings that allowed anyone with an internet connection to access them through Google and possibly other search engines. Alleged failings included failure to conduct an evaluation in response to the "environmental and operational changes" presented by implementation of the new server and conducting its risk assessments "in a patchwork fashion" that "did not result in an enterprise-wide risk analysis, as required by the HIPAA Security Rule."[8]

- **Catholic Health Care Services.** In June, HHS OCR announced that Catholic Health Care Services of the Archdiocese of Philadelphia, a business associate, agreed to pay $650,000 after an investigation prompted by the theft of an unencrypted iPhone without password protection exposed the PHI of 412 patients. HHS OCR alleged that CHCS "had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident." In the press release announcing the settlement, HHS OCR made a point of stating that it took the "unique and much-needed services" that CHCS provides into consideration, strongly suggesting that the penalty amount otherwise would have been even higher.[9]

- **U. Mass. Amherst.** In November, HHS OCR announced that the University of Massachusetts Amherst agreed to pay $400,000 after a malware infection resulted in the breach of the PHI of 1,670 individuals. Alleged failings included: not properly classifying part of its operations as being subject to HIPAA; failure to implement policies and procedures to comply with the Privacy and Security rules; failure to conduct an "accurate and complete" risk assessment; and failure to implement technical security measures, such as firewalls.[10]

- **Care New England Health System.** In September, HHS OCR announced that Care New England Health System (CNE) agreed to pay $400,000 after the loss of unencrypted backup tapes of a hospital for which CNE was acting as a business associate exposed the protected health information of approximately 14,000 patients. While the parties had a business associate agreement in place, it dated from 2005 and had not been updated to reflect changes required by the 2013 omnibus rule. HHS OCR did not take action with respect to the breach itself, finding that $150,000 settlement CNE had previously entered into with the Massachusetts Attorney General's office was sufficient for that aspect of the case.[11]

The seven settlements underscore several important points for all covered entities and business associates to review with counsel and with their privacy and data security teams:

- **Ensure (Current) Business Associate Agreements Are in Place.** It is necessary for covered entities to have a business associate agreement in place with each business associate and for business associates to have

5 http://www.hhs.gov/about/news/2016/07/21/ocr-announces-275-million-settlement-multiple-alleged-hipaa-violations.html
6 http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
7 http://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html
8 http://www.hhs.gov/about/news/2016/10/18/214-million-hipaa-settlement-underscores-importance-managing-security-risk.html
9 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html
10 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass
11 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wih

business associate agreements in place with each subcontractor that may create receive or maintain PHI. Having a business associate agreement is necessary (the OHSU and Advocate settlements included allegations that there was no business associate agreement in place at all), but it is not sufficient. The content of the business associate agreement that is in place also must reflect current HIPAA requirements. In the Care New England Health System case, for example, there was a business associate agreement, but it had not been updated since 2005. HHS OCR alleged that once the 2013 Omnibus Rule took effect, the PHI that CNE disclosed to its business associate under the out-of-date agreement was disclosed in violation of the Privacy Rule.

- **Conduct Comprehensive Risk Assessments.** The conduct and quality of risk assessments required by the HIPAA Security Rule are a repeated source of HHS OCR allegations of non-compliance. Not only must risk assessments be conducted, they must be comprehensive in scope and organizations need to address risk assessment findings of areas where remediation may be necessary. Inadequate risk assessments were at issue in a majority of the cases brought. It is important not only to conduct risk assessments, but to review the organization's operations to ensure that all operations involving PHI are included within the scope of the assessment. It also is important to HHS OCR that organizations take a comprehensive approach, faulting St. Joseph Health, for example, for conducting assessments which, in the agency's view, were done "in a patchwork fashion."

- **Review HIPAA Policies and Procedures.** Another recurring theme in recent HHS OCR actions is non-existent or inadequate policies and procedures for safeguarding PHI. In conjunction with risk assessments and other reviews, organizations should continue to implement and enhance their privacy and data security policies and procedures including, for example, policies restricting access to PHI and policies and procedures for responding to potential data breaches. Documenting privacy and security controls facilitates compliance with privacy rule requirements.

- **Review Specific Information Security Controls.** Breaches are the number one trigger for HHS OCR settlements. Taking steps to minimize the potential that a breach occurs in the first place, strengthens the organization's data security program, furthers compliance with the Security Rule (in the case of ePHI) and the Privacy Rule, and reduces the chances for an HHS OCR investigation. In the case of the breaches leading to the seven recent settlements discussed above, for example, alleged technical failings included: lack of encryption (e.g., back-up tapes, laptops, mobile phones); lack of access controls and audit trails; lack of firewalls; and lack of appropriate device configuration. Policies, procedures, and controls designed to prevent events that frequently result in breaches, such as lost or stolen back-up tapes, laptops or other devices with unsecured PHI and breaches due to file sharing software help reduce an organization's HHS OCR enforcement profile while also enhancing protections for PHI.

Authors and Contributors

Kevin Coy
Partner, DC Office
202.677.4034
kevin.coy@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/**