Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

HIPAA Enforcement: Lessons from the OCR's Recent Settlements

Publication — 10/26/2020

The OCR has announced a surprising number of HIPAA settlements in the past few months with penalties ranging from $10,000 to $6.5 million. Here are some of the key takeaways for healthcare providers:

1. Protect against cyberattacks. Healthcare entities remain a prime target for healthcare entities with disastrous effects for victims, including providers and patients whose information is compromised or destroyed. The HIPAA security rule is intended to ensure that healthcare entities maintain the integrity, availability and confidentiality of electronic protected heath information; successful cyberattacks often expose security rule violations. Premera Blue Cross agreed to pay $6.85 million after a phishing scam deployed malware that affected the information of 10.4 million persons. Another entity agreed to pay $2.3 million after a hacker accessed records of 6.1 million persons. Per the OCR, "The health care industry is a known target for hackers and cyberthieves. The failure to implement the security protections required by HIPAA Rules …. is inexcusable." https://www.hhs.gov/about/news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html. Cybersecurity is a major focus for HHS. In December 2018, the federal government published a guide to help healthcare providers of all sizes protect against cyberthreats, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, available at https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx. In July 2020, HHS launched its Health Sector Cybersecurity Coordination Center ("HC3") website, https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html, to offer additional support for healthcare providers. Cybersecurity is vital not only for regulatory compliance; it is essential to protect patients and ensure continued operation of the provider.

2. Perform an effective security risk assessment. The first and perhaps most important HIPAA security rule requirement is to perform an effective, enterprise-wide risk assessment of system vulnerabilities. The failure to perform and document an effective risk assessment is a frequently cited reason for HIPAA settlements with covered entities large and small. For example, a Utah physician agreed to pay $100,000 after failing to complete an accurate and thorough risk analysis or implement appropriate security measures despite receiving technical assistance. According to the OCR, "The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry." https://www.hhs.gov/about/news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html. In September 2020, CMS updated its Security Rule Assessment Tool—a free online resource

to help covered entities and business associates assess their risks and comply with security rule requirements. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. Covered entities and business associates should review and update their risk assessment on a regular basis, then follow up to address identified vulnerabilities.

3. Maintain appropriate policies and safeguards. The HIPAA privacy and security rules require covered entities to maintain appropriate policies and implement specified administrative, technical and physical safeguards. Business associates must also comply with security rule requirements. The failure to have required policies and safeguards in place not only exposes the covered entity or business associate to data breaches, but they may also evidence "willful neglect" resulting in mandatory HIPAA penalties. The absence of such policies and safeguards is, not surprisingly, a recurring factor in OCR settlements. In contrast, the OCR has suggested in commentary and seemingly practice that it will not usually seek penalties if the covered entity or business associate has the required policies and safeguards in place even if there is a breach. (*See* 75 FR 40879). For a list of required policies and safeguards, *see* https://www.hollandhart.com/pdf/HIPAA-Privacy-Checklist-HH.pdf and https://www.hollandhart.com/pdf/HIPAA-Security-Checklist-HH.pdf. Having the required policies will help protect against regulatory violations, but it is more important to ensure that the safeguards are effectively implemented to protect your patients' information and your own operations.

4. Encrypt your devices. The HIPAA security rule generally requires covered entities and business associates to encrypt devices containing protected health information. The theft or loss of unencrypted devices containing protected health information is presumptively a reportable breach and has repeatedly resulted in five- or six-figure settlements. For example, a Georgia ambulance company agreed to pay $65,000 following the loss of an unencrypted laptop containing information of 500 persons. A Rhode Island health system agreed to pay $1.04 million due to the theft of an unencrypted laptop containing the information of 20,431 individuals. And most recently, a New York hospital system agreed to a $3 million settlement due to the loss of an unencrypted laptop and flash drive containing information of an unspecified number of patients. The OCR stated, "Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk." https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html. HealthIT.gov has a website dedicated to protecting mobile devices: https://www.healthit.gov/topic/privacy-security-and-hipaa/your-mobile-device-and-health-information-privacy-and-security.

5. Respect the patient's right to access their information. The OCR is actively pursuing its initiative to enforce a patient's right to access their protected health information at a reasonable cost. Over the past year, the OCR has announced nine settlements ranging from $3,500 to $160,000 with a variety of providers. Under HIPAA, providers must:

a. Respond to patient requests to access their information within 30

days. In several of the reported cases, the providers delayed production for months despite repeated requests.

b. Provide all the records requested unless you fit within one of the limited exceptions that allows you to withhold records. (*See* 45 CFR 164.524). Several of the settlements involved situations in which the provider produced some but not all of the requested records despite repeated requests.

c. Provide the records in the form and format requested if readily producible, including electronic format.

d. Charge only a reasonable cost-based fee when producing records to the patient, *i.e*., the actual labor costs for copying the records, supplies, and postage. Providers may not charge additional retrieval or administrative costs. For more information on acceptable charges, *see* https://www.hollandhart.com/charging-patients-for-copies-of-their-records-ocr-guidance.

e. Produce requested records in a designated record set even if the records were created by or received from other providers. Contrary to common belief, HIPAA generally requires covered entities to produce all requested records in the designated record set regardless of who created them or where the records came from.

Settlements involving the right of access are usually lower than security violations due to the limited number of individuals involved. Nevertheless, the average settlement over the past year is still $63,500—a hefty sum, especially for small providers. The OCR has published a comprehensive guide explaining the patient's right to access, *Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524*, available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. All providers should review and understand the rules for access as interpreted by the OCR. As the OCR has noted, there really is no excuse for an access violation.

6. Respond promptly to known or suspected concerns.. In the vast majority of the reported settlements, the covered entity or business associate had prior notice of vulnerabilities but failed to take appropriate action to address them. In one case, the OCR had provided technical assistance following a prior similar incident but the same problems recurred. In another, the FBI had warned the entity that a hacker had targeted the entity but the entity left its records exposed for months. And in another, the covered entity disregarded the prior advice of the OCR. In most HIPAA cases, the OCR will look to resolve the matter by providing technical assistance and give the provider a chance to come into compliance; however, “[w]hen covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their negligence.” https://www.hhs.gov/about/news/2019/11/05/failure-to-encrypt-mobile-devices-leads-to-3-million-dollar-hipaa-settlement.html.

7. Report breaches in a timely manner. The breach notification rule requires covered entities to report breaches of unsecured health

information within 60 days unless there is a low probability that the data has been compromised. The OCR has warned that the failure to report the breach may constitute "willful neglect" triggering mandatory HIPAA penalties even if the underlying breach did not. (74 FR 40879). A Virginia hospital system agreed to pay $2.175 million because it failed to timely self-report a breach. Per the OCR, "When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by the OCR." https://www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html.

8. Business associates beware! HIPAA applies directly to business associates as well as healthcare providers and health insurers. Last year, the OCR listed the HIPAA violations for which business associates may be directly liable. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html. In September, a business associate agreed to pay $2.3 million for failing to implement security measures after a hacker accessed over 6 million patient records.

9. Small providers are not exempt. "All health care providers, large and small, need to take their HIPAA obligations seriously." https://www.hhs.gov/about/news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html. Many of the settlements involving access violations involved relatively small physician practices. As discussed above, a Utah gastroenterologist agreed to pay $100,000 for security rule violations. A North Carolina FQHC agreed to pay $25,000 for systemic security rule noncompliance. And a small Texas dental practice had to pay $10,000 for improperly disclosing protected health information in response to a social media post. Which leads to the next lesson…

10. Do not disclose PHI on social media. Covered entities may not disclose protected health information on social media in response to a patient's post without the patient's HIPAA-compliant authorization. Protected health information includes any information if "there is a reasonable basis to believe the information can be used to identify the individual." (45 CFR 160.103). Any information that indicates the person is a patient is protected. As the OCR stated, "Doctors and dentists must think carefully about patient privacy before responding to online reviews." https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html.

Conclusion. Given the thousands of HIPAA complaints or breach reports that the OCR must receive annually, very, very few actually result in penalties or settlements; they are usually reserved for fairly egregious cases involving repeated or complete disregard of HIPAA obligations. Even if they experience a breach, covered entities and business associates can generally avoid HIPAA penalties if they can document their good faith compliance, including performing and regularly updating an appropriate security risk assessment; implementing appropriate policies and safeguards such as encryption; training personnel; and responding promptly and appropriately to suspected violations. As the recent

enforcement actions show, the OCR is willing to go after providers and business associates who ignore their HIPAA obligations.
