NEXSEN | PRUET

HIPAA Enforcement Remains Strong in 2020

Related Professionals

Shannon V. Lipham
803.540.2155
SVLipham@nexsenpruet.com

Practices

Health Law

10.26.2020

It seems like every aspect of healthcare is changing during these uncertain times, but one thing remains the same – HIPAA enforcement is going strong. The Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS), responsible for enforcing HIPAA regulations, has been active this year in terms of settlements of potential HIPAA privacy and security violations. More than $12.2 million has been recorded this year in resolution agreements, despite the Notification of Enforcement Discretion related to COVID-19 issued by HHS.

HIPAA settlements have affected almost every sector of the health industry including insurers, physician clinics and solo practitioners, an FQHC, and business associates, to name a few. Here's a summary of OCR's HIPAA settlements in 2020 thus far:

Right of Access

- For the first time, it appears that OCR's Right of Access Initiative, announced in 2019 to enforce patients' rights to timely access to their medical records at a reasonable cost, has been on the front burner. There have been seven settlements just this year and nine in total.
- The most recent settlement involved NY Spine Medicine, a private medical practice specializing in neurology and pain management, which agreed to pay $100,000 and take corrective actions to resolve a potential violation of the right of access standard. The investigation occurred after OCR received a complaint from an individual alleging she had made multiple requests to NY Spine Medicine for her medical records, and that she did not receive all the requested records. Click here to see the HHS press release.
- Also earlier this month, OCR settled with a large acute care hospital in Phoenix, AZ for $160,000 based on potential right of access violations. Similarly, the investigation stemmed from a complaint filed with OCR by a mother alleging she made multiple requests to the hospital for her son's records as his personal representative, and the hospital did not provide all of the requested records. Click here to see the HHS press release.

Cyber Attacks and Stolen Information

- The two largest settlements this year involved health insurers. Anthem, Inc., an Indianapolis, IN-based health insurer settled with state attorneys general in 43 states for $39.5 million, based on an investigation into the largest health data breach in history. Back in 2018, Anthem settled with OCR for $16 million and agreed to take substantial corrective action to settle the potential HIPAA violations related to this data breach. Click here to see the HHS press release.
- Earlier this year, Premera Blue Cross, the largest health plan in the Pacific Northwest, settled with OCR for $6.85 million and to implement a corrective action plan. The settlement stemmed from a cyber attack on Premera Blue Cross's system through malware and a phishing email, exposing over 10.4 million individuals' electronic protected health information. Click here to see the HHS press release.
- In July, an Athens, GA based orthopedic clinic settled with OCR for $1.5 million and is required to implement a corrective action plan to settle potential HIPAA violations. Back in 2016, the clinic was notified that a database of their patient records may have been posted for sale online. A few days later, a hacker contacted the clinic demanding money in return for a complete copy of the database. The clinic determined the database had been stolen using a vender's credentials to access their electronic medical record system. The breach affected over 200,000 individuals, and disclosed PHI including patients' names, dates of birth, social security numbers, medical procedures, test results, and health insurance information. Again, OCR's investigation found a failure to conduct a risk analysis and implement risk management controls, and a failure to secure business associate agreements with multiple business associates. Click here to see the HHS press release.
- CHSPSC, LLC, a company providing a variety of business associate services including IT and health management information to hospitals and physician clinics in Franklin, TN, agreed in September to pay $2.3 million based on a potential HIPAA breach affecting over 6 million people. The company was notified in 2014 by the FBI of a cyberhacking group's persistent threat to CHSPSC's information system, but nonetheless hackers continued to access the protected health information of 6,121,158 individuals over a three-month span through remote access. OCR's investigation revealed "longstanding, systemic noncompliance" with HIPAA. Click here to see the HHS press release.
- In June, a nonprofit health system in Rhode Island agreed to pay $1.04 million and adopt a corrective action plan to settle potential violations of the HIPAA privacy and security rules related to a hospital employee's unencrypted laptop that was stolen. The large settlement is based on a determination by OCR that there had been "systemic noncompliance" with the HIPAA rules, including a failure to encrypt protected health information on laptops, a lack of device and media controls, and a failure to have a business associate agreement in place with the nonprofit's parent company. Click here to see the HHS press release.

Small Providers

- In February, the practice of a Utah gastroenterologist and solo practitioner was determined by OCR to have demonstrated significant noncompliance with HIPAA. The investigation began after a breach report was filed with OCR related to a dispute with a business associate. Specifically, OCR found that the practice failed to conduct any risk analysis, and "failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." Click here to see the HHS press release, which emphasizes the importance of a "thorough risk analysis and risk management plan."

→ In July, a small Federally Qualified Health Center (FQHC) providing services in rural North Carolina settled with OCR for $25,000 to resolve potential HIPAA violations. The FQHC filed a breach report in 2011 due to an impermissible disclosure of protected health information to an unknown email account, resulting in a breach that affected 1,263 patients. OCR's investigation determined the FQHC had "longstanding, systemic noncompliance with the HIPAA security rule," including that it failed to implement any HIPAA policies and procedures and "neglected to provide workforce members with security awareness training until 2016." Click here to see the HHS press release.

Recent HIPAA enforcement actions serve as a reminder that all covered entities and business associates – no matter the size – need to constantly be taking steps to ensure HIPAA compliance. Otherwise, covered entities and business associates risk potential enforcement, the consequences of which can be extremely costly and negatively impact reputation.