HIPAA Violations: What Providers Should Learn From the Failures of Others

March 4, 2024

The federal agency responsible for enforcing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) - the Office of Civil Rights (OCR) at the U.S. Department of Health and Human Services - recently submitted two reports to Congress outlining the agencies HIPAA enforcement activities in 2022. The reports provide a helpful roadmap for health care provider compliance activities related to the protected health information (PHI) that they create, receive, maintain, or transmit during normal operations.

Each report covers a different aspect of OCR's role in HIPAA enforcement. One report discusses breaches of unsecured PHI and the other is focused on HIPAA "Privacy, Security, and Breach Notification Rule Compliance." In 2022, OCR reports that it collected $2.4 million in payments related to breaches and $3.3 million in payments related to HIPAA complaints and investigations. The vast majority of these financial penalties were paid by health care providers and entities.

Breaches of Unsecured Protected Health Information

OCR received more than 64,000 notifications of breaches in 2022. The vast majority of the breaches affected less than 500 individuals, but more than 600 separate breaches affected more than 500 people (overall, these large breaches impacted more than 40 million people). This volume of breaches reflects a moderate increase over the previous year in large breaches and this increase continues a trend of increases as OCR notes that the number of breaches affecting 500 of more individuals rose 107% between 2018 and 2022.

HIPAA defines a "breach" at 45 C.F.R. § 164.402 as the "acquisition, access, use, or disclosure of PHI in a manner not permitted by [the HIPAA Privacy Rule] which compromises the security or privacy of the PHI." HIPAA Covered Entities and Business Associates are required to report breaches affecting 500 or more people to the federal government "without unreasonable delay" but smaller breaches need not be reported until the end of the calendar year. The Covered Entity must also report the breach to the affected individuals and in some cases the media. Following notice, OCR will conduct an investigation of large breaches and if it determines that the Covered Entity was not in compliance with HIPAA, the Covered Entity may be subject to corrective action plans, resolution agreements, payment of a monetary settlement amount, or a Civil Money Penalties (CMP).

OCR noted in the report that hacking and IT incidents caused almost 75% of large breaches. The next most common cause was unauthorized access or disclosure by Covered Entity personnel which accounted for 19% of the breaches. Data theft, loss, and improper disposal caused most of the remaining.

Complaints Alleging HIPAA Violations

Under HIPAA, OCR is also responsible for investigating potential violations of HIPAA by Covered Entities and Business Associates even when such violation did not cause a breach. An OCR investigation is typically triggered by either third-party complaints submitted to OCR alleging a violation of HIPAA or because OCR becomes aware of an incident on its own through breach notifications, media stories, or referrals from other government entities. OCR classifies incidents from the former as Complaints and the latter as "Compliance Reviews."

OCR received more than 30,000 complaints in 2022 but 87% were resolved by OCR without any investigation. OCR notes that complaints that do not result in investigations include complaints against entities that are not subject to HIPAA or that alleged conduct that did not violate HIPAA.

The vast majority of the rest of the complaints (9%) were resolved with technical assistance. As a result, only a small portion of third-party complaints are resolved through invasive methods including written resolution agreements, corrective action plans, monetary settlements, and/or civil money penalties. On the other hand, Compliance Investigations are much more likely to lead to corrective actions. OCR completed 846 Compliance Reviews in 2022 and 80% of the investigated entities were required to take corrective action or pay a civil money penalty.

Lessons for Providers from the OCR Reports

The Annual OCR reports provide an excellent resource for HIPAA Covered Entities and their advisors on how to better comply with the requirements of the law. Each report provides insight into OCR's enforcement process, common sources of HIPAA issues, and ways to mitigate or reduce HIPAA risks. The reports nicely summarize the common traps that lead to HIPAA issues. According to OCR, the most common sources of HIPAA violations include:

- Ransomware that compromised health care provider servers;
- Malware;
- Phishing;
- Unauthorized Posting of PHI to public websites;
- Unauthorized use of data tracking technologies;
- Employees impermissibly accessing records;

- Misdirected communications; and
- Theft of Laptops containing PHI

The reports also outline steps that may have been missed by Covered Entities that led to OCR scrutiny. Reviewing these "missed steps" and making improvements to organizational resources can substantially reduce the risk of HIPAA failures. In reviewing the OCR reports, three major themes are evident in HIPAA failures: poor technology utilization, poorly trained staff, and failure to adopt simple organization policies and procedures. To reduce the chances of a HIPPA issue, Covered Entities and Business Associates should consider the following steps:

- Technology Enhancements. A significant number breaches could be avoided if health care providers adopted more aggressive technical safeguards to protect data. These include requiring multi-factor authentication for employee access to PHI, expanding the use of encryption technologies especially when sending PHI electronically, and requiring more frequent password changes for those with access to PHI.
- Training Personnel. The number of breaches can also be reduced by expanding efforts to reduce human error. This includes training (and re-training) of workforce members who handle PHI. Workforce training may touch on a number of issues including appropriate handling of PHI, rules related to PHI disclosures, and how to avoid hacks through expansion of education on malware, phishing, and other email-based hacking processes. It is also important to train personnel to respond to requests for PHI from patients in a timely manner as some of the largest financial penalties assessed by OCR in 2022 were the result of a health care provider's failure to respond to a valid request for medical records.
- Organizational Strategies. Many breaches may also be prevented through improved organizational processes including effective privacy officers, effective risk and vulnerability assessments, and robust review of information security activity. For example, a basic requirement of HIPAA Covered Entities is to appoint a privacy officer but in a number of cases review by OCR, the HIPAA entity had either failed to appoint a privacy officer or the privacy officer was not properly qualified to perform the duties assigned. HIPAA health care providers are also required to assess potential risks and vulnerabilities but even in cases where the HIPAA entity conducted the assessment, it was often found to be substandard. OCR noted that many risk assessments failed to prevent breaches because the assessment reviewed incomplete information including neglecting to review locations where PHI is created, received, maintained, or transmitted. Providers should also be performing a more robust review of information security activity including audit logs, access reports, and security incident tracking reports and ensuring the procedural mechanisms used to prevent unauthorized access are up to date.

If you have questions about HIPAA compliance in the health care industry or the OCR's new reports, or you need help reviewing your current HIPAA practices and procedures, please contact Ben Peltier, or any member of the Lathrop GPM Health Law practice group.