Now & Next
Healthcare Alert

November 13, 2024

OCR enforcement and outreach emphasizes HIPAA security compliance

By Valerie Breslin Montague and Philip Cramer[i]

Trends taken from OCR's ransomware-related enforcement remind HIPAA-regulated organizations to implement security best practices.

What's the impact?

- Four new ransomware HIPAA enforcement actions highlight compliance concerns beyond simply a cyberattack.
- Though compliance investigations may take time, HIPAA-regulated entities can glean lessons from prior enforcement and guidance to strengthen compliance programs.
- OCR's new Risk Analysis Initiative and updated Security Risk Assessment Tool emphasize the importance of a compliant HIPAA security risk analysis.

In September and October 2024, the US Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced four enforcement actions with covered entity healthcare providers for alleged HIPAA violations involving ransomware attacks, bringing the total number of ransomware-related enforcement actions to seven. OCR describes how large HIPAA breaches,

those impacting 500 or more individuals, that involve ransomware attacks have increased by 264% since 2018. A number of trends emerge from OCR's recent enforcement actions, as well as other recent OCR outreach.

First Risk Analysis Initiative enforcement

Designed to increase "better compliance" with the HIPAA security risk analysis requirement, a compliance concern cited by OCR in numerous enforcement actions, OCR launched a new Risk Analysis Initiative. On October 31, 2024, OCR announced its seventh enforcement action related to ransomware and its first under its Risk Analysis Initiative. Bryan County Ambulance Authority (BCAA), a county-owned emergency medical services provider in Oklahoma, submitted a breach notification to OCR on May 18, 2022, describing how a ransomware incident encrypted files on BCAA's network. The encrypted files impacted the protected health information (PHI) of 14,273 patients. OCR determined that BCAA did not conduct a compliant risk analysis, and BCAA agreed to pay $90,000 and comply with a three-year corrective action plan (CAP).

As it sees a number of ransomware trends in its cybersecurity investigations, OCR also released a video capturing some best practices and guidance for addressing ransomware and other cybersecurity threats. Addressing HIPAA security risk analyses, Nicholas Heesters, the Senior Advisor for Cybersecurity at OCR, mentions that "OCR's HIPAA investigations frequently find non-compliant risk analysis and risk management processes as a contributing factor in many breaches." While HIPAA-regulated entities are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to electronic PHI (ePHI), Mr. Heesters acknowledges that "accurate" and "thorough" are not defined in the HIPAA regulations but states that "accurate generally means being correct and thorough generally means being comprehensive." He continues that an accurate and thorough risk analysis will consider risks to all of an organization's ePHI. OCR frequently finds a lack of thoroughness in an organization's risk analyses, such as the inclusion of only a subset of the organization's environment in its analysis of the risks posed to ePHI or a lack of comprehensiveness in considering the risks posed by technical vulnerabilities. The new OCR initiative, as well as its continued guidance on the importance of compliant security risk analyses, provides a clear directive to healthcare providers, health plans, and all other HIPAA-regulated entities that the lack of a comprehensive security risk analysis may be a significant issue if the organization is investigated following a ransomware attack.

On November 1, 2024, OCR and the Assistant Secretary for Technology Policy released an updated version of the OCR/Office of the National Coordinator for Health Information Technology Security Risk Assessment Tool. Although developed to assist smaller healthcare organizations with identifying and assessing potential risks and vulnerabilities to ePHI, any organization can use the content to advise its security risk analysis process, and this can be a helpful starting point for organizations seeking to prepare a compliant security risk analysis for the first time.

Post-transaction compliance for HIPAA-regulated entities

OCR kicked off Cybersecurity Awareness Month on October 3, 2024, by announcing a $240,000 civil monetary penalty (CMP) against Providence Medical Institute (PMI) following an investigation of PMI's ransomware-related breach. PMI, a nonprofit physician services organization providing care across Southern California, reported a breach to OCR on April 18, 2018, impacting the medical records of approximately 85,000 individuals. PMI acquired an orthopedic medical practice, the Center for Orthopaedic Specialists (COS), in July 2016. PMI informed OCR that, post-transaction, it intended to integrate COS into its information technology (IT) platform. Before it could do so, but more than a year and a half after the acquisition transaction, a COS workforce member clicked on a phishing email, leading to the encryption of COS' systems via ransomware technology on February 18, 2018. Two additional ransomware attacks occurred on February 25, 2018, and March 4, 2018, respectively.

Through its investigation, OCR determined that PMI did not have a business associate agreement in place with its IT vendor until June 2018, after OCR commenced its compliance investigation of PMI. The OCR investigation also determined that approximately three months following the ransomware attacks, PMI performed an assessment of COS's environment, which found, among other issues, that COS hosted ePHI on unsupported and obsolete operating systems, it did not have a demilitarized zone network separating its private network from public and untrusted networks, its firewall was not configured to monitor and track access or network changes, and COS workforce members shared generic, administrator-level credentials. Given the consistency of mergers and acquisitions in the healthcare space, many HIPAA-regulated entities are or will be faced with the challenge of onboarding a new affiliate. While there are many considerations involved in that process, the PMI enforcement action is a reminder to make HIPAA compliance and cybersecurity a priority, both in the transaction diligence process and in the post-transaction integration.

Entities investigated by OCR should carefully analyze informal resolution versus CMPs

As indicated in the OCR Notice of Proposed Determination, OCR offered PMI the opportunity to resolve the allegations of HIPAA noncompliance informally outside of the CMP process as it concluded its investigation. OCR then sent PMI a Letter of Opportunity that informed PMI of its alleged HIPAA violations and OCR's attempts to pursue an informal resolution. PMI provided a response, which OCR determined did not support an affirmative defense. Analyzing a potential mitigating factor provided by PMI, as well as aggravating factors from its investigation, OCR determined that PMI did not justify a CMP waiver and issued its Notice of Proposed Determination, which acknowledges that PMI had Recognized Security Practices in place, which reduced the amount of the CMP by twenty percent. There may be a benefit to a HIPAA-regulated entity in declining to accept an OCR offer for informal resolution of alleged HIPAA violations. For example, the issuance of a CMP does not include a CAP, which, as indicated above, can result in

a three-year compliance review and reporting process. On the flip side, HIPAA noncompliance spanning a significant length of time, or multiple noncompliance issues, can result in a costly CMP. Resolving identified issues through an OCR settlement or other informal process may result in a lower payment for the HIPAA-regulated entity, and the continued improvements to HIPAA compliance through the CAP process may not only result in more robust compliance but may provide OCR with deep knowledge of the entity's focus on security if the entity were to experience a future data incident or complaint.

Data backup is key

OCR announced a settlement with Plastic Surgery Associates of South Dakota, Ltd. (PSASD) on October 31, 2024, following a July 27, 2017, breach report that nine PSASD workstations and two servers were infected with ransomware impacting approximately 10,229 individuals. After its investigation concluded that PSASD demonstrated "significant noncompliance" with the HIPAA requirements, the parties agreed to a $500,000 settlement and a two-year CAP. OCR learned that PSASD was unable to restore its impacted servers from backup and that it paid ransom to the threat actor to secure decryption keys. OCR found multiple alleged HIPAA violations, including the failure to conduct a compliant security risk analysis, the failure to implement sufficient security measures, and the failure to implement policies and procedures to regularly review information system activity and to address security incidents.

As part of its CAP, PSASD must create and implement policies and procedures to create and maintain backup copies of its ePHI, regularly test that these backups are recoverable, create and maintain multiple copies of encrypted backups, and securely store them in different locations. Lack of recoverable backup data is not only a HIPAA compliance issue; it can have catastrophic impacts on patient care and operations. The PSASD settlement is a reminder to healthcare organizations to not only ensure that data backups are in place but to test them, securely store them, and train workforce members on these processes.

Not all ransomware investigations are triggered by breach notifications

On September 26, 2024, OCR published a June 2024 HIPAA settlement involving a ransomware attack on Cascade Eye and Skin Centers, P.C. (Cascade), a healthcare provider treating eye and skin issues in Washington. This settlement is notable because OCR's investigation did not commence following a breach notification from Cascade, but rather, it was triggered by a complaint alleging that Cascade experienced a ransomware attack. OCR's investigation determined that approximately 291,000 files with ePHI had been impacted in the attack. In its investigation of Cascade, OCR identified potential HIPAA noncompliance, including the failure to conduct a compliant risk analysis of potential risks and vulnerabilities to ePHI, as well as insufficient monitoring of health information system activity. As part of its Resolution Agreement

with OCR, Cascade must pay $250,000 and comply with a two-year CAP. HIPAA-regulated organizations experiencing a ransomware attack should ensure that they comply with any required breach reporting obligations and remember that, even if the event does not trigger breach reporting, the entity may not escape compliance review.

HIPAA breach investigations and corresponding resolution efforts may take time

Addressing a ransomware attack can be daunting, and the uncertainty of the timing of governmental investigations and litigation can be stressful. However, as with many OCR compliance investigations that do not involve ransomware, OCR investigations and the process for informal resolution or a CMP often take time. Analyzing the following recent ransomware-related enforcement actions indicates that HIPAA-regulated entities may need to prepare for a multi-year process.

PMI

- Investigation—OCR notified PMI of its investigation on May 10, 2018
- Enforcement—Notice of Final Determination issued July 1, 2024
- Length—More than six years

BCAA

- Investigation—OCR notified BCAA of its investigation on June 9, 2022
- Enforcement—Resolution Agreement executed July 29, 2024
- Length—More than two years

PSASD

- Investigation—OCR initiated investigation following receipt of PSASD's breach report on July 27, 2017
- Enforcement—Resolution Agreement executed May 3, 2024
- Length—Almost seven years

CASCADE

- Investigation—OCR received complaint regarding Cascade on May 26, 2017
- Enforcement—Resolution Agreement executed June 17, 2024
- Length—More than seven years

Organizations benefit from robust HIPAA compliance programs

While an organization may be unable to prevent ransomware attacks, a robust HIPAA compliance program may eliminate or lessen OCR enforcement.

As evidenced in each of these enforcement actions, a ransomware attack alone is not the reason for OCR enforcement. In each investigation, OCR found other HIPAA violations, including a lack of a business associate agreement, a non-compliant security risk analysis, and a lack of data backup. HIPAA-regulated entities should continuously work to ensure that their compliance program addresses the needs of current systems and operations and that workforce members are trained on the compliance aspects of their particular job functions.

Using the examples from recent HIPAA enforcement, as an organization looks to enhance its security protocols, it needs to consider the human element as well. OCR issued an October 2024 Cybersecurity Newsletter focused on the use of social engineering to conduct cyberattacks, such as when an unauthorized individual learns information on a target individual via their social media accounts and uses that information to trick them into revealing system credentials. OCR emphasizes that simply implementing security tools will not eliminate cyber threats. It is important for healthcare organizations to train workforce members on how to identify phishing attacks, how to avoid downloading malicious software via smishing attacks conducted via text message, and how to detect attackers using artificial intelligence (AI) to create deepfakes that mimic a person's image or voice. A multi-faceted approach to HIPAA compliance positions a HIPAA-regulated entity in a strong stance to defend against and respond to ransomware and other cyberattacks.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

[i] Philip Cramer (Legal Intern—Healthcare practice) assisted with the preparation of this alert.