PUBLICATION

Insider Threats Are Just as Dangerous as Ransomware – Lessons from the Latest OCR HIPAA Settlement

Authors: Layna S. Cook Rush, Alisa L. Chestler
June 04, 2025

What's New?

On May 28, 2025, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced an $800,000 settlement with a large Florida-based health care provider over potential violations of the HIPAA Security Rule stemming from insider misuse of access credentials. According to the press release, the incident involved a former non-clinical employee of a physician's practice who retained access to the health system's electronic medical record (EMR) system and allegedly used that access to inappropriately view and share a patient's protected health information (PHI).

OCR's investigation found that the health system failed to implement appropriate policies and procedures to authorize and manage user access, did not reduce risks and vulnerabilities to a reasonable level, and lacked regular audit reviews of system activity – all required under the HIPAA Security Rule. These gaps made the organization vulnerable not only to an external cyberattack but also to an insider with credentials accessing information beyond their authority.

Who's Feeling the Impact?

This enforcement action affects:

- Covered entities and business associates across the health care industry, especially those who provide system access to unrelated entities and must rely on the security and privacy practices of another health care provider or business associate.

Why Should Health Care Providers Care?

This case serves as a reminder: data breaches are not always the work of external actors or ransomware, insider threats – including former or low-level personnel with unlimited or lingering access – can be just as damaging. Health care organizations must remain vigilant not only against outside attackers but also against risks from within. Moreover, the amount of the settlement payment – $800,000 – for what appears to be a potential snooping case seems to indicate OCR's concern with oversight of affiliated provider groups and business associates.

What's Your Next Move?

- **Conduct a thorough and ongoing risk analysis** to identify where electronic PHI (ePHI) resides in your IT environment and how it flows through your systems, including how it is accessed by health care partners and business associates.

- **Implement role-based access controls** and regularly review and revoke access for terminated or transferred personnel, health care partners, and business associates.
- **Maintain and regularly review audit logs** to monitor access and detect unauthorized behavior.
- **Provide regular, role-specific HIPAA training** to all workforce members. Require health care partners and business associates do the same.
- **Encrypt ePHI in transit and at rest** and use authentication mechanisms to prevent unauthorized access.

The full OCR resolution agreement and corrective action plan can be found here. More guidance on securing ePHI is available via NIST's HIPAA Security Rule toolkit.

Bottom line: Insider threats are real, and regulators are watching. Privacy and security programs must account not only for outside threats like ransomware but also the risk of internal misuse or mismanagement of access to sensitive health data.

For more information or assistance on this topic, please contact Layna Cook Rush, CIPP/US, CIPP/C, Alisa L. Chestler, CIPP/US, QTE, Hannah Moore, or a member of Baker Donelson's Health Information Technology team.

Hannah Moore, a summer associate at Baker Donelson, contributed to this article.