Insights

HIPAA Wrapped: OCR's 2024 HIPAA Highlights

February 3, 2025

By: Stacy Walton Long and Thomas M. Abrams

OCR Director Melanie Fontes Rainer released an announcement on January 7, 2025 recapping OCR's HIPAA accomplishments and enforcements in 2024. ("Announcement"). In the Announcement, Rainer highlights new rules implemented and enforcement actions taken by her agency in 2024. Covered entities should review, and likely supplement, existing processes and policies to comply with these recently adopted rules under HIPAA.

Rulemaking

In 2024, OCR set an annual record for HIPAA rulemaking as it issued two final rules and one proposed rule. To align 42 CFR Part 2 closer with HIPAA's Privacy, Breach Notification, and Enforcement Rules, OCR published the Confidentiality of Substance Use Disorder (SUD) Patient Records Final Rule in February 2024. The "Part 2 Final Rule" delivered important synergies for covered entities and business associates handling both Part 2 and non-Part 2 records, who now may rely on a single consent for all future uses and disclosures for treatment, payment, and health care operations ("TPO"). Where covered entities and business associates receive Part 2 records based on such a consent, the Part 2 Final Rule permits redisclosure in accordance with HIPAA. OCR also replaced previous Part 2 penalties with those applicable under HIPAA, and applied the HIPAA breach notification requirements to breaches involving Part 2 records.

In April 2024, OCR created new protections for protected health information ("PHI") potentially related to reproductive health care (e.g., STIs, prenatal care, abortion). The Reproductive Health Care Final Rule, codified at 45 CFR Part 160 and 164, prohibits the use or disclosure of PHI for the purposes of investigating or penalizing individuals for seeking, obtaining, providing, or facilitating lawful reproductive care. Where PHI related to reproductive health is requested for health oversight activities, judicial or administrative proceedings, law enforcement purposes, or to inform a coroner or medical examiner about a decedent, the requestor *must provide* a signed attestation that the request is not for a prohibited purpose before the covered entity may disclose the PHI.

OCR also proposed HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information (90 Fed. Reg. 898) in December 2024, to clarify and update the HIPAA Security Rule based on modern cybersecurity best practices consistent with the National Institute of Standards and Technology ("NIST"). If finalized as proposed, the rule will eliminate the distinction between "addressable" and "required" implementation specifications, making all implementation specifications mandatory with few exceptions. The scope of administrative, technical, and physical safeguards would also expand to demand more from covered entities. Business associates will also be required to notify covered entities within 24 hours of (1) the

termination of a workforce member's access to ePHI (or relevant electronic information system), or (2) activation of a contingency plan. Annually, covered entities will be required to verify the technical safeguards of their business associates. How the forthcoming final rule will vary from the proposed rule remains to be seen but, barring a significant overhaul, the Security Rule will be more robust in 2025.

Enforcement

The 22 enforcement actions completed by OCR in 2024 were the second most in OCR history and resulted in almost $10 million in settlements and civil money penalties. Ransomware, phishing, impermissible access to ePHI, impermissible disclosures of reproductive health information, untimely patient access to PHI, and unsecured PHI left on the internet, were subjects of enforcement emphasized by OCR. Enforcement activity is unlikely to plateau in 2025 as OCR begins to enforce three additional rules, subject to the yet uncertain impact of the new Trump Administration.

Considerations for Covered Entities and Business Associates

To reflect what we saw from OCR in 2024, covered entities and business associates should consider the following actions:

- Review and adjust policies and training to reflect the alignment of Part 2's consent requirements and breach notification protocol with HIPAA.
- Update policies to reflect the new reproductive health care rules and train appropriate personnel to understand when PHI is related to reproductive health, the types of requestors who must provide an attestation in order to obtain reproductive health PHI, and what purposes are "prohibited purposes" for which reproductive health PHI may not be disclosed.
- Survey existing security safeguards based on the proposed HIPAA Security Rule to strengthen the cybersecurity of ePHI and lay the groundwork for improvements and updates likely to be required pending the final rule.

OCR's productive 2024 means a busy 2025 for covered entities, all of which could change under the new Trump Administration. Please reach out to Stacy Walton Long, Thomas M. Abrams, or any member of the Krieg DeVault Health Care Practice to address questions related to this Alert.
