2024 HIPAA Regulations Update



ARTICLE 09.30.24 KEVIN CORNWELL

Updating HIPAA regulations is a gradual process, starting with feedback requests from the Department of Health and Human Services (HHS) to address outdated or burdensome aspects of the law. Following this, a Notice of Proposed Rulemaking (NPRM) is issued, inviting industry comments before a Final Rule is released. Significant changes proposed for 2024 include changes to the HIPAA Privacy Rule and new requirements for patient access to their Protected Health Information (PHI).

Notably, the timeframe for responding to access requests is shortened, and mandates around electronic health records are clarified. Although these updates aim to streamline processes, they pose implementation challenges for healthcare organizations, including necessary training and policy adjustments. Additionally, the HHS plans to propose new cybersecurity regulations by the end of 2024 to bolster patient data protection amid rising cyber threats.

Recent and Proposed Changes

Proposed New HIPAA Privacy Rule Changes

- Patients can inspect their PHI in person and take notes or photos.
- Access to PHI must be provided within 15 days (reduced from 30).
- Transfers of ePHI to third parties are limited to what's in an EHR.
- Individuals can request PHI transfers to personal health applications.
- Individuals should receive ePHI at no cost in certain situations.
- Covered entities must inform individuals of their rights regarding PHI summaries.
- Estimated fee schedules for PHI access must be posted online.
- Individualized fee estimates for PHI copies are required.
- A pathway is created to direct the sharing of PHI among entities.
- Providers must respond to records requests directed under the HIPAA Right of Access.
- The requirement for written confirmation of privacy notice provision is removed.
- PHI can be disclosed to prevent reasonably foreseeable threats to health or safety.
- Certain uses of PHI can be made in good faith for the individual's best interest.
- A minimum necessary standard is established for care coordination disclosures.
- The definition of healthcare operations now includes care coordination.
- Armed Forces can use or disclose PHI to all uniformed services.

- A definition for electronic health records is added.

Transaction Code Set Update Adds Three New Codes to enable electronic transmission of healthcare attachment transactions

HHS Healthcare Sector Cybersecurity Strategy Report

1. Establish voluntary cybersecurity goals for the healthcare sector
2. Provide resources to incentivize and implement cybersecurity practices
3. Implement an HHS-wide strategy to support greater enforcement and accountability
4. Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity

In 2019, OCR maintained robust enforcement efforts, concluding the year with 10 settlements and civil monetary penalties amounting to $12,274,000. Toward the end of the year, OCR launched a new initiative to ensure compliance with the HIPAA Right of Access, which mandates that individuals receive timely access to their medical records for a reasonable, cost-based fee.

Penalty Structure for HIPAA Violations in 2024

Annual Penalty Limit	Annual Penalty Limit	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of knowledge	$137	$34,464	$34,464
Tier 2	Reasonable cause	$1,379	$68,928	$137,886
Tier 3	Willful neglect	$13,785	$68,928	$344,638
Tier 4	Willful neglect (not corrected within 30 days)	$68,928	$68,928	$2,067,813