

## HHS Issues Proposed Rule to Modify HIPAA Security Rule

Source: Alliance Daily | Dec. 30, 2024

On Friday, December 27, the U.S. Department of Health and Human Services (HHS) Office of Civil Rights released a [Notice of Proposed Rulemaking](#) to amend the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This proposed rule would propose significant changes intended to improve cybersecurity standards for the protection of electronic protected health information (ePHI). This is in response to an evolving healthcare landscape, characterized by an alarming increase in cyberattacks and cybersecurity breaches occurring nationwide in the healthcare sector. HHS has published a [press release](#) and [fact sheet](#) with information on topline proposals accompanying the proposed rule. Comments on the proposed rule are due March 7, 2025.

The Security Rule,[\[1\]](#) part of the HIPAA regulations,[\[2\]](#) was initially published in 2003 and last modified in January 2013. It creates standards for protecting the confidentiality and integrity of ePHI, and applies to covered entities—including health plans, healthcare clearinghouses, and healthcare providers—that create, receive, maintain, or transmit ePHI.

The proposed rule addresses significant changes in technology, changes in breach trends and cyberattacks, HHS' Office for Civil Rights' (OCR's) enforcement experience, and other guidelines, best practices, methodologies, procedures, and processes for protecting ePHI. In addition, the proposed rule addresses the following topics, including a request for comments in each section:

- **Updating Definitions:** The proposed rule clarifies and updates terminology used in a non-exhaustive list of examples of electronic storage material, including preparing for future technology. It also includes updates to reflect the role of emerging technologies, such as artificial intelligence (AI) and quantum computing in data security.
- **Security Standards:** HHS proposes improving consistency of language between the Security Rule and other sections of HIPAA, by including more flexibility and scalability.
- **Administrative Safeguards:** HHS proposes to update policies and procedures for the management and execution of security measures, including requirements for risk analyses that incorporate testing and evaluation of security measures.
- **Physical Safeguards:** The proposed rule would modify Security Rule physical safeguard standards and addresses recent case law regarding steps to protect confidentiality, integrity, and availability of ePHI.

- **Technical Safeguards:** The proposed rule aims to improve guidance to ensure covered entities are adequately implementing, reviewing, and updating their policies and procedures, and includes, among other things, requirements for encryption and multi-factor authentication (MFA) to safeguard ePHI.
- **Organizational Requirements:** HHS proposes adding additional requirements to business associate agreements and when to activate contingency plans, to address risk trends and contingency planning for data breaches and service interruptions.
- **Documentation Requirements:** HHS proposes to delete and modify documentation requirements to align with administrative, physical, and technical safeguards changes throughout this proposed rule by requiring written documentation to be in electronic form. In addition, the rule would modify specifications for documentation time limits, availability, and updates.
- **Transition Provisions:** HHS proposes to remove compliance date information in 45 CFR 164.318 and replace this language for transitioning to the revised Security Rule, if finalized.
- **New and Emerging Technologies Request for Information (RFI):** HHS is requesting information on quantum computing, AI, virtual and augmented reality (VR and AR) and its impact on the Security Rule.

The Alliance is working on a more detailed breakdown of the proposed rule as well as scheduling opportunities for members to provide feedback. If you have feedback or questions, please reach out to [regulatory@allianceforcareathome.org](mailto:regulatory@allianceforcareathome.org).