epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

`COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Health and Human Services

on

Notice of Proposed Rulemaking:
HIPAA Security Rule to Strengthen the Cybersecurity of
Electronic Protected Health Information

90 Fed. Reg. 898

March 7, 2025

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Department of Health and Human Services (HHS)'s January 6, 2025 request for comment on its notice of proposed rulemaking to modify the Security Standards for the Protection of Electronic Protected Health Information (Security Rule) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).[1] The proposed modifications would improve the cybersecurity of electronic protected health information (ePHI) by revising existing standards to better protect the confidentiality, integrity, and availability of ePHI.[2] EPIC commends HHS for taking meaningful steps to protect the security of patients' ePHI to keep pace with modern technologies and digital practices and to protect against ever-increasing data security incidents.

[1] Request for Comment on HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (Jan. 6, 2025) [hereinafter HIPAA Security Rule NPRM].
[2] *Id*.

Modernizing the HIPAA Security Rule is important to ensure that HIPAA is effective today and in the future.

EPIC is a public interest research center in Washington, D.C. established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC routinely files comments in response to proposed rulemakings concerning the protection of personal information. EPIC has advocated for strong data security and cybersecurity protections to protect the privacy of individuals' personal information and has played a leading role in developing regulatory authority to address emerging privacy and cybersecurity issues.[3] EPIC has also urged that businesses and other entities be required restrict their collection, use, disclosure, and retention of sensitive personal information, such as protected health information, to that which is strictly necessary.[4]

Cybersecurity is crucial to protecting patients. With the increased digitization of health care—including telehealth, online booking of appointments, digital charts, and electronic health records—the risk of data security incidents has increased dramatically. Patients' most sensitive health information is vulnerable to cyberattacks, unauthorized disclosure, and breaches. HIPAA is

[3] EPIC & CFA, Comments to the CPPA on Proposed Regulations Regarding Cybersecurity, Risk Assessments, and ADMTs (Feb. 19, 2025), https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/; EPIC, et al., Reply Comments in Cybersecurity Labeling for Internet of Things (Nov. 10, 2023), https://epic.org/documents/reply-comments-in-cybersecurity-labeling-for-internet-of-things/; EPIC, Comments to the FTC on Proposed Rulemaking to Amend the Health Breach Notification Rule (Aug. 8, 2023), http://epic.org/documents/epic-comments-to-the-ftc-on-proposed-rulemaking-to-amend-the-health-breach-notification-rule/; In re Implementation of the Telecommunications Act of 1996, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, CC Docket. No. 96-115, RM-11277 (Aug. 30, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513325075.

[4] *See, e.g.*, John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too* (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/; EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; EPIC & Consumer Report, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

intended to protect patient information, but the Security Rule has lagged behind technological innovation and emerging threats. Cybersecurity breaches have an outsized impact on individuals; people whose data have been lost to a breach are more susceptible to identity theft and financial fraud, and many suffer psychological harms such as anxiety, depression, and PTSD.[5] HHS should set a high floor that will lead to more robust, uniform data security across the health care sector.

Many of the proposed updates reflect best cybersecurity practices that regulated entities should have already adopted; HHS should finalize these requirements without hesitation. For example, the proposed regulations eliminate the distinction between "addressable" and "required" implementation specifications.[6] This change makes all of the implementation specifications mandatory with specific, enumerated exceptions—and rightly so, as the addressable implementation specifications were never meant to be optional. This change is essential to enable effective enforcement of the Security Rule and to hold entities to rigorous data security standards. Further, the proposed rulemaking requires stronger technical and administrative safeguards consistent with modern cybersecurity practices. These include multifactor authentication, network segmentation, and data encryption. These requirements reflect baseline cybersecurity measures to protect against data security incidents. Indeed, health care entities should already be taking these steps to protect their patients.

---

[5] *See, e.g.*, Danielle Citron & Daniel Solove, *Risk and Anxiety: A Theory of Data Breach Harms*, Texas L. Rev. (2018), https://scholarship.law.bu.edu/faculty_scholarship/616/; Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021,* DOJ, Doc. No. NCJ 306474 at 12 (Oct. 2023) https://bjs.ojp.gov/document/vit21.pdf; Ido Kilovaty, *Psychological Data Breach Harms*, U.N.C. J. of L. & Tech. (2021), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1432&context=ncjolt; Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA Today (Feb. 24, 2020), https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/; Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, Info. Sec. (Sep. 12, 2016), https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/.

[6] HIPAA Security Rule NPRM, *supra* note 1, at 933.

Other requirements in the NPRM are essential to protect the security of ePHI. The proposed rulemaking would mandate routine review and testing of security measures, technology asset inventory and risk analysis, and contingency planning. As proposed in the NPRM, covered entities that implement security measures to protect patients' sensitive information should be required to routinely review and test the measures to ensure they are working properly and their efficacy, and to modify the measure when appropriate and reasonable. The NPRM also makes clear that a covered entity should further be required to conduct a technology asset inventory to determine the location of data it maintains and to conduct a risk analysis to detect potential vulnerabilities and risks. As the NPRM aptly explains, "Regulated entities cannot understand the risks to the confidentiality, integrity, and availability of their ePHI without a complete understanding of these assets."[7]

Further, an entity should not collect or maintain sensitive health information if it cannot identify where the data is stored, and it must be able to determine its vulnerabilities to prevent against unauthorized access. Data mapping is a practice that ensures that a company understands the scope of what it must protect and the way it should respond when its security measures have failed to prevent a breach. As privacy Professors Solove and Hartzog have explained:

> Privacy requirements such as data mapping provide awareness about potential security vulnerabilities. Data mapping shows what data is being collected and maintained, the purposes for having this data, the whereabouts of this data, and other key information.[8]

The proposed updates further require that each covered entity establish a contingency plan to respond to unexpected adverse events that threaten the confidentiality, integrity, and availability of ePHI.[9] Data security incidents include breaches, which are on the rise: 2024 had a record-breaking

[7] HIPAA Security Rule NPRM, *supra* note 1, at 937.
[8] Daniel J. Solove & Woodrow Hartzog, *Breached! Why Data Security Law Fails and How to Improve It*, 156-57 (2022), Oxford University Press 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4173764.
[9] HIPAA Security Rule NPRM, *supra* note 1, at 955.

275 million breached health records and the largest-ever health care data breach.[10] This type of plan helps regulated entities respond to unforeseen events quickly, mitigating harms to the business and patients. This includes emergencies like fire, a cyberattack, or system failure, during which an entity will not be equipped to create and implement a plan. This is a best practice to mitigate damage during an emergency.

In conclusion, we applaud HHS for undertaking updates the HIPAA Security Rule to better protect patients' sensitive ePHI. These improvements are essential to make HIPAA's protections effective in the digital age and to raise the floor for the security of health information across all covered entities.

Respectfully Submitted,

/s/ *John Davisson*
John Davisson
Director of Litigation & Senior Counsel

/s/ *Sara Geoghegan*
Sara Geoghegan
EPIC Counsel

[10] Steve Alder, *Healthcare Data Breach Statistics*, HIPAA Journal (Jan. 20, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/.