



NEW DEVELOPMENTS IN HEALTH INFORMATION PRIVACY AND SECURITY LAW

Presented by:

Adam Greene, Partner, Davis Wright Tremaine LLP, Washington, DC
Christopher Finch, Vice President, Chief Compliance and Audit Officer
MemorialCare, Long Beach, CA

1

Agenda



- HIPAA Amendments to Further Safeguard Reproductive Health Care
- HIPAA Security Rule Notice of Proposed Rulemaking
- Website Disclosures of Health Information
- Confidentiality of Substance Use Disorder Patient Records amendments
- State Consumer Data Laws
- FTC Enforcement of Health Privacy
- Increased Interoperability and Increased Breach Risks

2

HIPAA Amendments to Further Safeguard Reproductive Health Care

□ □ □ □ □

3

Reproductive Health Care Amendments



- Final rule on April 26, 2024.
- Compliance deadline of December 23, 2024.
 - Delayed February 16, 2026, deadline for amending notice of privacy practices.
- On December 5, 2024, HHS Office for Civil Rights (OCR) announced that it was committed to enforcing the amendments.

4

Reproductive Health Care Amendments



- Prohibition on using or disclosing protected health information (PHI) to investigate or impose liability on seeking, obtaining, providing, or facilitating lawful reproductive health care.
- Attestation of permitted purpose for uses and disclosures for health oversight activities, judicial and administrative proceedings, law enforcement, and (for decedents) coroners and medical examiners.
- Changes to HIPAA notice of privacy practices.

Current Challenges with 2024 Amendments



- Requestors, including federal agencies, are refusing to sign attestations.
- How do you limit when an attestation is requested:
 - Limit based on scope of PHI
 - Limited based on nature of request

Potential Future



- OCR and state attorneys general (AGs) vigorously enforce the amendments.
- OCR silently does not enforce amendments (AGs can still enforce).
- HHS stops defending rule in court cases and lets courts vacate the amendments.
- OCR issues notice of enforcement discretion (AGs can still enforce).
- OCR withdraws amendments through notice-and-comment rulemaking.

Reproductive Health Care Amendments



- Three cases:
 - *Purl, M.D. et al v. United States Department of Health and Human Services et al*, Docket No. 2:24-cv-00228 (N.D. Tex. Oct 21, 2024)
 - *State of Texas v. United States Department of Health and Human Services et al*, Docket No. 5:24-cv-00204 (N.D. Tex. Sep 04, 2024)
 - *State of Tennessee et al v. U.S. Department of Health and Human Services et al*, Docket No. 3:25-cv-00025 (E.D. Tenn. Jan 17, 2025)

Reproductive Health Care Amendments



- Preliminary injunction against HHS enforcing the 2024 amendments against physician and her practice (Purl, 12/22/24).
- HHS alleges that defendants have no standing in all three cases.
- 3/13/25 brief (Tennessee) – “HHS’s new leadership is currently reviewing the Rule.”
- 5/12/25 brief (Purl) – “[D]efendants respectfully inform the Court that the Rule remains among a number of agency actions from the prior administration that are under consideration at HHS, but given other agency priorities, no imminent action on the Rule is expected.”

Epilogue



On June 18, 2025, the N.D. Tex. vacated the 2024 rule (except for notice of privacy practices changes related to 42 C.F.R. part 2) in *Purl v. HHS*.

- Held that plaintiffs had standing due to regulatory burden.
- Held that 2024 rule violated HIPAA statute by limiting public health activities (child abuse reporting) that HIPAA does not preempt.
- Also applying major-questions doctrine to find that HHS’ broad authority to promulgate privacy standards does not extend to addressing major questions like abortion.
- Vacated rule nationally.
- HHS has 60 days to appeal.

HIPAA Security Rule Notice of Proposed Rulemaking

□ □ □ □ □

11

Security Rule NPRM



- Eliminates “addressable” implementation specifications – all would be required.
- More detailed requirements, such as inventory of technology assets, network map, patch management with 15-day deadline, 1-hour deadline for terminating employee access, etc.
- Requires encryption and multifactor authentication with very limited exceptions.
- Requires business associates to agree to 24-hour notification of activation of contingency plan.
- Requires dozens of actions to be done on an annual basis.

12

Security Rule NPRM



- Proposed on January 6, 2025.
- Comments due on March 7, 2025.
- 4,747 comments received.
- Finalization of the rule as proposed seems unlikely.

898 Federal Register / Vol. 90, No. 3 / Monday, January 6, 2025 / Proposed Rules

DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office of the Secretary

45 CFR Parts 160 and 164

HHS-0945-A22
HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

Abstract: Office for Civil Rights (OCR), Office of the Secretary, Department of Health and Human Services.

ACTION: Notice of proposed rulemaking notice of Tribal consultation.

SUMMARY: The Department of Health and Human Services (HHS or "Department") is issuing this notice of proposed rulemaking (NPRM) to solicit comment on its proposal 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). The proposed modifications would revise existing standards to better protect the confidentiality, integrity, and availability of electronic protected health information (ePHI). The proposals in this NPRM would increase the cybersecurity for ePHI by revising the Security Rule to address changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates (collectively, "regulated entities"); other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.

DATES:
Comments: Submit comments on or before March 7, 2025.
Meeting: Pursuant to Executive Order 13757, Consultation and Coordination with Indian Tribal Governments, the Department of Health and Human Services will hold a meeting for the Tribal consultation meeting for the Docket ID number HHS-OCR-0945-A22. Follow the instructions at <https://www.regulations.gov> for submitting electronic comments. Attachments should be in Microsoft Word or Portable Document Format (PDF).

FOR FURTHER INFORMATION CONTACT: Maria Goshen-Nguyen at (202) 240-2118 or (800) 368-7468 (TDD), or by email at OCRPrivacy@hhs.gov.

SUPPLEMENTARY INFORMATION: The discussion below includes an Executive Summary, a description of relevant statutory and regulatory authority and history, the justification for this proposed regulation, a section-by-section description of the proposed modifications, and a regulatory impact analysis and other required regulatory analyses. The Department solicits public comment on all aspects of the proposed rule. The Department requests that persons commenting on the provisions of the proposed rule label their discussion of any particular provision or topic with a citation to the section of the proposed rule being addressed and identify the particular request for comment being addressed, if applicable.

Table of Contents

1. Executive Summary
A. Overview
B. Applicability
C. Table of Abbreviations/Commonly Used Acronyms in This Document
D. Statutory Authority and Regulatory History
1. Statutory Authority and History
2. Health Information Technology for Economic and Clinical Health (HITECH) Act
B. Regulatory History
1. 1996 Security Rule Notice of Proposed Rulemaking
2. 2003 Final Rule
3. 2009 Description of Authority
4. 2013 Omnibus Reauthorizing Legislation
III. Justification for This Proposed Rulemaking
A. Strong Security Standards Are Essential to Protecting the Confidentiality, Integrity, and Availability of ePHI and Ensuring Quality and Efficiency in the Health Care System
B. The Health Care Environment Has

Website Disclosures



HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for...  [A-Z Index](#)

 **HIPAA for Individuals**  **Filing a Complaint**  **HIPAA for Professionals**  **Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance Materials](#) > Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

HIPAA for Professionals Text Resize [A](#) [A](#) [A](#)  Share   

Regulatory Initiatives

Privacy 

- Summary of the Privacy Rule
- Guidance
- Combined Text of All Rules
- HIPAA Related Links

Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities¹ and business associates² ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").³ OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities' noncompliance with the HIPAA Rules. A regulated entity's failure to comply with the HIPAA Rules may result in a civil money penalty.⁴

15 | New Developments in Health Information Privacy and Security Law | June 2025

 AMERICAN HEALTH LAW ASSOCIATION

15

AHA sues HHS Over Online Tracking Guidance (November 2023)

- AHA joined by Texas Hospital Association, Texas Health Resources, and United Regional Health Care System
- Seeks declaratory judgment
- Alleges bulletin exceeds statutory authority
- Alleges HHS's website is inconsistent with bulletin

2/9/24, 10:23 AM Hospital associations and hospitals file lawsuit challenging federal rule that ties providers' hands in efforts to reach communities

 American Hospital Association

1/23 / News (December/January 2024) / Headline (December/January 2024)

Hospital associations and hospitals file lawsuit challenging federal rule that ties providers' hands in efforts to reach communities

© Nov 02, 2023 - 04:01 PM



The AHA, joined by the Texas Hospital Association, Texas Health Resources, and United Regional Health Care System, Nov. 2 sued <https://www.ahr.org/news/press-releases/2023/11/02/calls-complaints-aha-its-its-united-health-care-systems-calls-the-federal-government-to-see-enforcement-of-an-unlawful-harmful-and-counterproductive-rule-that-has-suspended-hospitals-and-health-systems-ability-to-share-health-care-information-with-the-communities-they-serve-analyze-their-own-websites-to-enhance-accessibility-and-improve-public-health>

<https://www.ahr.org/news/press-releases/2023/11/02/calls-complaints-aha-its-its-united-health-care-systems-calls-the-federal-government-to-see-enforcement-of-an-unlawful-harmful-and-counterproductive-rule-that-has-suspended-hospitals-and-health-systems-ability-to-share-health-care-information-with-the-communities-they-serve-analyze-their-own-websites-to-enhance-accessibility-and-improve-public-health>

16 | New Developments in Health Information Privacy and Security Law | June 2025

 AMERICAN HEALTH LAW ASSOCIATION

16

OCR Updates Guidance on Online Tracking (Mar. 18, 2024)



- Focuses on intent of website visitor.
 - Student visiting hospital's oncology webpage to write term paper is not PHI about student.
 - Individual visiting same page to seek a second opinion on treatment options for a brain tumor is PHI.
- Indicates an enforcement priority on whether Security Rule risk analysis addresses website disclosure risks.

AHA wins lawsuit (June 20, 2024)



- “Simply put, Identity (Person A) + Query (Condition B) \neq IIHI (Person A has Condition B).”
- Declared the guidance unlawful and vacated with respect to the “Proscribed Combination” of “circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a [unauthenticated public webpage] addressing specific health conditions or healthcare providers.”
- Does not seek to declare the remainder of the guidance unlawful.
- OCR updated its bulletin, indicating that “HHS is evaluating its next steps in light of [the] order.”

Largest threat remains class action lawsuits:



LOCAL NEWS

NC hospital system settles patients Meta Pixel lawsuit for \$6.6 million

Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for \$18.4 Million

Advocate Aurora settles pixel suit for \$12M

Naomi Diaz - Thursday, August 17th, 2023

Confidentiality of Substance Use Disorder Patient Treatment Records



42 C.F.R. Part 2



- Applies to:
 - Federally-assisted “programs”:
 - Specialty facilities or individuals who hold themselves out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment (“SUD services”);
 - Identified unit within general medical facility that holds itself out as providing, and provides, SUD services; or
 - Medical personnel or other staff within general medical facility whose primary function is provision of SUD services and is identified as such a provider.
 - Qualified service organizations (service providers)
 - Lawful holders (receive SUD records pursuant to a consent)
- More stringent than HIPAA with respect to limits on uses and disclosures of SUD records

February 2024 Final Rule



- Revises 42 C.F.R. Part 2 (“Part 2 Rule”) terms to be more consistent with HIPAA (e.g., “use and disclosure” throughout)
- Revises Part 2 Rule’s consent requirement to make more consistent with HIPAA
- Permits patient to provide one-time authorization for all uses and disclosures of Part 2 Records for treatment, payment, and health care operations (“TPO”)
- HIPAA-regulated recipient of Part 2 Records generally can further use and disclose as permitted under HIPAA [Limited to records received pursuant to TPO consent?]

February 2024 Final Rule (continued)

- Patient right to an accounting of disclosures
- Applies HIPAA Breach Notification Rule to Part 2 Rule
- Applies HIPAA criminal and civil enforcement mechanisms to Part 2 Rule
- Prohibits use or disclosure of Part 2 Records for civil, criminal, administrative, or legislative proceeding against the patient



February 2024 Final Rule (continued)



- Likely impact:
 - Continued need to segregate data
 - Increased risk of enforcement
- Remaining question: If patient provides limited consent, can CE/BA recipient use and disclose to the extent permitted by HIPAA?
- Compliance date:
February 16, 2026

State Consumer Data Privacy Laws

□ □ □ □ □

25

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
California	\$25M or 100,000 CA residents	Yes (in hands of CE/BA)	No	Generally yes	Jan. 1, 2020
Colorado	100,000 CO residents	Yes (in hands of CE/BA)	No	No	July 1, 2023
Connecticut	100,000 CT residents	Yes	Yes	Yes	July 1, 2023
Delaware	35,000 DE residents	Yes	No	No	Jan. 1, 2025
Florida	\$1B and smart speaker or app store	Yes	Yes	Yes	July 1, 2024
Indiana	100,000 IN residents	Yes	Yes	Yes	Jan. 1, 2026
Iowa	100,000 IA residents	Yes	Yes	Yes	Jan. 1, 2025

26

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
Kentucky	100,000 KY residents	Yes	Yes	Yes	Jan. 1, 2026
Maryland	35,000 MD residents	Yes	No	No	Oct. 1, 2025
Minnesota	100,000 MN residents	Yes	No	No	July 31, 2025
Montana	50,000 MT residents	Yes	Yes	Yes	Oct. 1, 2024
Nebraska	Processes or engages in sale of personal data	Yes	Yes	Yes	Jan. 1, 2025
New Hampshire	35,000 NH residents	Yes	Yes	Yes	Jan. 1, 2025
New Jersey	100,000 NJ residents	Yes	No	Yes	Jan. 15, 2025

States with General Privacy Laws

State	Threshold*	PHI Exempt	CE/BA Exempt	Nonprofits Exempt	Date
Oregon	100,000 OR residents	Yes (processed by CE/BA)	No	No	July 1, 2024
Rhode Island	35,000 RI residents	Yes	Yes	Yes	Jan. 1, 2026
Tennessee	\$25M and 175,000 TN residents	Yes	Yes	Yes	July 1, 2025
Texas	Process or engage in sale of personal data	Yes	Yes	Yes	July 1, 2024
Utah	\$25M and 100,000 UT residents	Yes	Yes	Yes	Dec. 31, 2023
Virginia	100,000 VA residents	Yes	Yes	Yes	Jan. 1, 2023

State Consumer Health Privacy Laws



- Passed in Washington, Nevada, and Connecticut, with New York awaiting Governor's signature.
- Consent requirements for collection of consumer health data (CHD) other than to deliver requested product or service.
- Strong notice requirements (WA AG requires separate CHD notice)
- Strong transparency requirements (e.g., listing of third-party recipients)
- Strong privacy rights (such as right of deletion without exception)

FTC Enforcement of Health Privacy



Recent Health Information Privacy Enforcement

- Cases under Section 5 of the FTC Act, primarily over website visitor disclosures.
- First enforcement actions under Health Breach Notification Rule (“HBNR”).
- Also used Opioid Addiction Recovery Fraud Prevention Act to obtain civil monetary penalties in website disclosure cases.

Potential Future



- Section 5 Enforcement (For-profit entities)
 - Likely to lessen; and
 - More straightforward cases, less envelope-pushing.
- HBNR
 - Republican commissioners previously objected to expanded interpretation.
 - Continue to enforce?
 - Silently stop enforcing?
 - Revert to more narrow statutory interpretation through notice-and-comment rulemaking?

Increased Interoperability and Increased Breach Risks



33

Federal Interoperability Efforts

- Trusted Exchange Framework and Common Agreement (“TEFCA”) – nationwide health information exchange framework
- 21st Century Cures Act Information Blocking Prohibition
- Promoting Interoperability Program Application Programming Interface (“API”) requirements

34

Breach Notification

- HIPAA requires a covered entity to notify affected individuals, HHS, and potentially the media of a breach of unsecured PHI.
- A breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule.
 - Certain exceptions, but none based on noncompliance of another entity.
- 2008 guidance (pre-Breach Notification Rule): “a covered entity is not liable for a disclosure that is based on the non-compliance of another entity within the health information exchange, as long as the covered entity has complied with the Privacy Rule.”

Breach Notification Costs

- Reputational harm
- Potential litigation defense
- Cost of notifications
- Cost of credit monitoring
- Cost of call center
- Potential regulatory investigation
- Costs of responding to breach

Epic v. Particle Health



In its notice, Epic said its 15-member Care Everywhere Governing Council flagged three companies, who are Particle Health customers, for questionable use of patient data not related to patient care or treatment. One of these companies, Integritort, provides legal professionals with access to real-time medical records, according to the company's website. Another healthcare organization planned to file a formal dispute with Carequality alleging that Integritort used the health data networks to get medical information "for the apparent purpose of identifying potential participants in class action lawsuits while claiming a Permitted Purpose of Treatment," Epic said in its notice.



Whose Breach?

- One argument:
 - Disclosure by "good" participant in violation of Privacy Rule, even if not their fault.
 - Policy Reason: Patients know and trust "good" participant so more likely to take such notification seriously.
 - Policy Reason: "Bad" participant may not be subject to HIPAA and, therefore, may not have HIPAA breach notification obligations.

Whose Breach?

- Counter argument:
 - Disclosure was for a permitted purpose (e.g., treatment) based on “good” participant’s understanding.
 - The “bad” participant made had the breach because they used the PHI for an impermissible purpose.
 - Lack of applicability of HIPAA can be addressed through contractual breach notification requirements.
 - Policy Reason: Holding “good” participant responsible for breach will have a chilling effect on health information exchange participation.

Whose Breach?

- TEFCA
 - Requires compliance with breach notification law, but silent on who has what responsibility.
- HHS Office for Civil Rights
 - Informally seems leaning towards treating the breach responsibilities as falling on “good” participant.
 - Has not responded to formal letter requesting clarification.

Questions

Adam Greene
Partner, Davis Wright Tremaine
LLP
adamgreene@dwt.com

Christopher Finch
Vice President, Chief
Compliance and Audit Officer,
MemorialCare
cfinch@memorialcare.org



© 2025 is published by the American Health Law Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America.

Any views or advice offered in this publication are those of its authors and should not be construed as the position of the American Health Law Association.

“This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought” —from a declaration of the American Bar Association.