Davis Wright Tremaine LLP

DWT.COM

New Developments in Health Information Privacy and Security Law

Fall 2025 Privacy+Security Forum

Adam Greene

Partner | Washington, D.C.

Friday, November 14, 2025

Agenda

- HIPAA Amendments to Further Safeguard Reproductive Health Care
- Other HIPAA Privacy Rule Changes
- HIPAA Security Rule Notice of Proposed Rulemaking
- Website Disclosures of Health Information
- Immigration Enforcement and Patient Privacy
- AI and Health Data
- Confidentiality of Substance Use Disorder Patient Records Amendments
- State Health Information Privacy Laws
- FTC Enforcement of Health Privacy

HIPAA Amendments to Further Safeguard Reproductive Health Care

Davis Wright Tremaine LLP

2024 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 (with respect to both reproductive health care and substance use disorder records).

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 with respect to reproductive health care and substance use disorder records.
- On December 5, 2024, HHS Office for Civil Rights (OCR) announced that it was committed to enforcing the amendments.

Purl Decision (June 18, 2025)

- 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 applied 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 (except for notice of privacy practices changes related to substance use disorder records governed by 42 C.F.R. part 2).
- HHS had 60 days to appeal (deadline of August 17, 2025).

After *Purl* Decision

- Trump v. CASA limited national injunctions by district courts but did not impact the *Purl* decision: “Nothing we say today resolves the distinct question whether the Administrative Procedure Act authorizes federal courts to vacate federal agency action. See 5 U. S. C. §706(2) (authorizing courts to “hold unlawful and set aside agency action”).”
- HHS did not appeal, confirming no intent to do so on September 2, 2025.
- City of Columbus, OH, Doctors for America, City of Madison, WI:
  - Sought to intervene on January 17, 2025;
  - Court denied intervention request on April 15, 2025;
  - On June 13, 2025, proposed intervenors appealed denial of intervention request to Fifth Circuit;
  - On August 15, 2025, proposed intervenors appealed court’s vacating of the 2024 amendments to Fifth Circuit; and
  - On September 4, 2025, interveners filed an unopposed motion to dismiss their appeal (“Defendants have chosen not to appeal the District Court’s Summary Judgment Orders, and Movants-Appellants have concluded that the resources of the parties and the courts would be best conserved by dismissing this appeal.”); and
  - On September 10, 2025, Fifth Circuit dismissed appeal.

Other HIPAA Privacy Rule Changes

2021 Proposed Privacy Rule Amendments

- Right of Access
  - Shorter deadline
  - Reconcile with *Ciox Health* decision (limiting 3rd party directives to e-copies of EHR PHI)
  - Requires CEs to submit right-of-access requests on individuals' behalf

2021 Proposed Privacy Rule Amendments

- Improvements to care coordination
  - Revision to definition of “health care operations”
  - Disclosures to community-based organizations
  - Exception to minimum necessary for health plan’s case management and care coordination

2021 Proposed Privacy Rule Amendments

- Miscellaneous
  - Eliminate acknowledgment of notice of privacy practices
  - “Professional judgment” becomes “good faith belief” in several places
  - “Serious and imminent” becomes “reasonably foreseeable harm”
  - Disclosures to telecommunications relay services
  - Disclosures to uniformed services personnel
- HHS is seeking to finalize in May 2026

HIPAA Security Rule Notice of Proposed Rulemaking

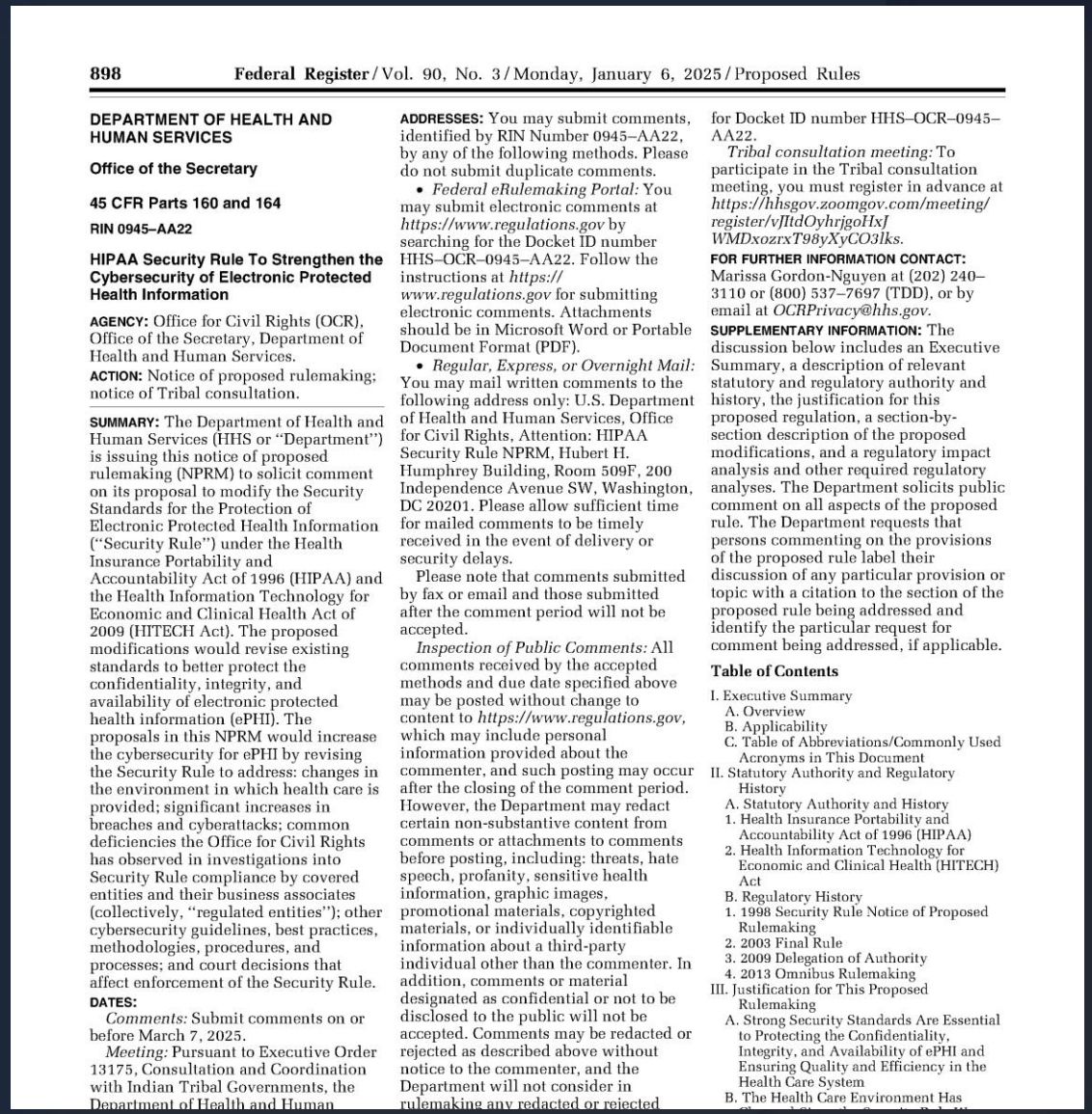
Davis Wright Tremaine LLP

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.

Security Rule NPRM

- Proposed on January 6, 2025.
- Comments due on March 7, 2025.
- 4,747 comments received.
- HHS is seeking to finalize rule in May 2026. Finalization of *all* proposed provisions 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

RIN 0945–AA22

HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information

AGENCY: 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 13175, Consultation and Coordination with Indian Tribal Governments, the Department of Health and Human

ADDRESSES: You may submit comments, identified by RIN Number 0945–AA22, by any of the following methods. Please do not submit duplicate comments.

- *Federal eRulemaking Portal:* You may submit electronic comments at *https://www.regulations.gov* by searching for the Docket ID number HHS–OCR–0945–AA22. Follow the instructions at *https://www.regulations.gov* for submitting electronic comments. Attachments should be in Microsoft Word or Portable Document Format (PDF).
- *Regular, Express, or Overnight Mail:* You may mail written comments to the following address only: U.S. Department of Health and Human Services, Office for Civil Rights, Attention: HIPAA Security Rule NPRM, Hubert H. Humphrey Building, Room 509F, 200 Independence Avenue SW, Washington, DC 20201. Please allow sufficient time for mailed comments to be timely received in the event of delivery or security delays.

Please note that comments submitted by fax or email and those submitted after the comment period will not be accepted.

Inspection of Public Comments: All comments received by the accepted methods and due date specified above may be posted without change to content to *https://www.regulations.gov*, which may include personal information provided about the commenter, and such posting may occur after the closing of the comment period. However, the Department may redact certain non-substantive content from comments or attachments to comments before posting, including: threats, hate speech, profanity, sensitive health information, graphic images, promotional materials, copyrighted materials, or individually identifiable information about a third-party individual other than the commenter. In addition, comments or material designated as confidential or not to be disclosed to the public will not be accepted. Comments may be redacted or rejected as described above without notice to the commenter, and the Department will not consider in rulemaking any redacted or rejected

for Docket ID number HHS–OCR–0945–AA22.

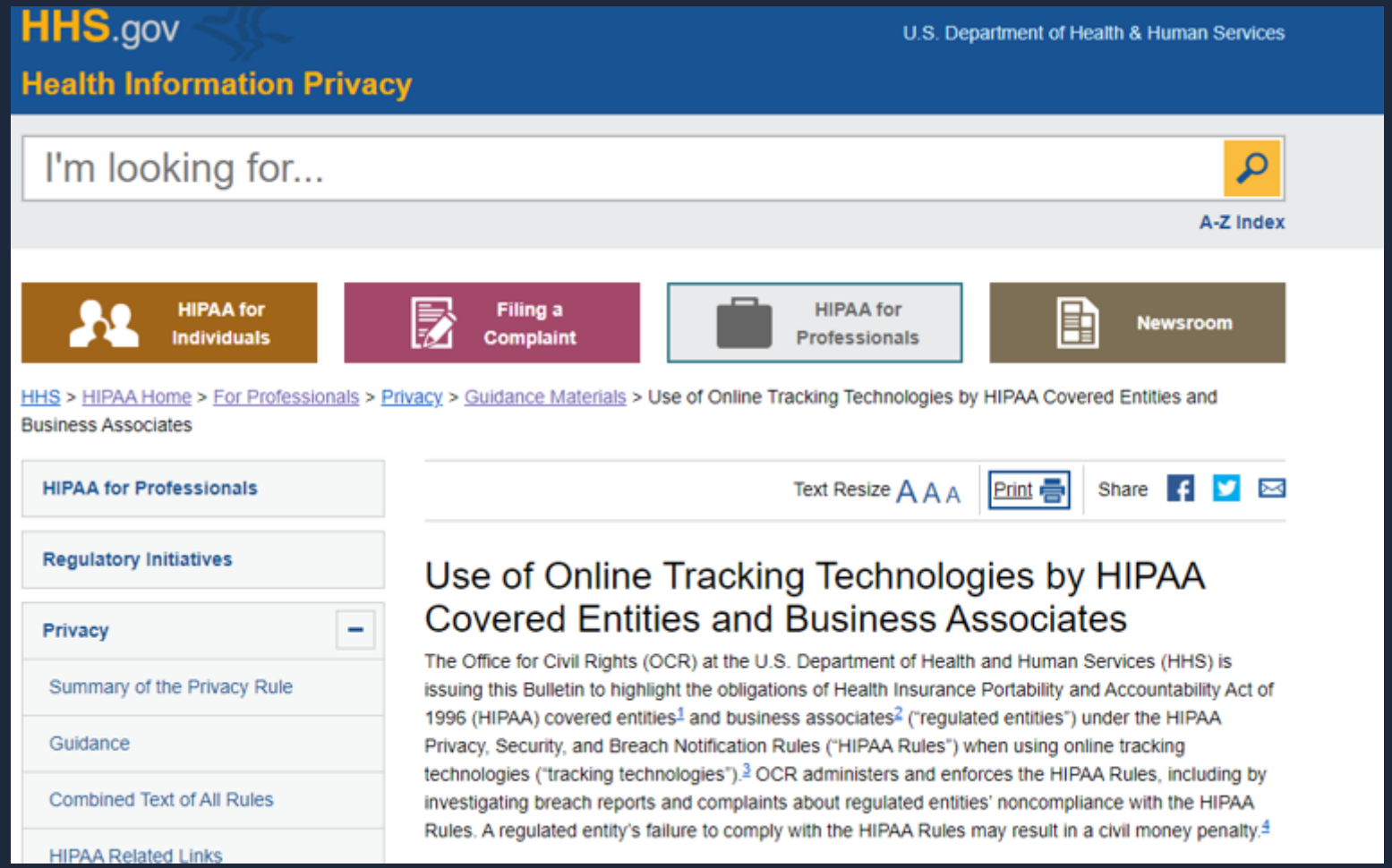
Tribal consultation meeting: To participate in the Tribal consultation meeting, you must register in advance at *https://hhsgov.zoomgov.com/meeting/register/vJItdOyhrjgoHxJWMDxozrxT98yXyCO3lks.*

FOR FURTHER INFORMATION CONTACT: Marissa Gordon-Nguyen at (202) 240–3110 or (800) 537–7697 (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

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
Regulatory Initiatives
Privacy
Summary of the Privacy Rule
Guidance
Combined Text of All Rules
HIPAA Related Links
Text Resize A A A
Print
Share
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 entities[1] and business associates[2] ("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]

AHA wins lawsuit (June 20, 2024)

- “Simply put, Identity (Person A) + Query (Condition B) ≠ 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

Immigration Enforcement and Patient Privacy

Davis Wright Tremaine LLP

General HIPAA Issues

- **Scope of "protected health information" (PHI)** – includes mere fact that someone is a patient.
- **Definition of "disclosure"** – includes "provision of access to" information, but it is not clear whether failing to block federal agents from entering treatment areas constitutes "provision of access to" any resulting PHI.
- **Reasonable safeguards** – a covered entity must implement reasonable safeguards to prevent impermissible uses and disclosures of PHI, but is it reasonable to block a federal agent from entering a treatment area?

HIPAA Guidance on Access to Media

https://www.hhs.gov/hipaa/for-professionals/faq/2023/film-and-media/index.html

- Does not address disclosures to law enforcement but can be read as generally restricting third parties' facility access.
- "The HIPAA Privacy Rule does not require health care providers to prevent members of the media from entering areas of their facilities that are otherwise generally accessible to the public, which may include public waiting areas or areas where the public enters or exits the facility."
- "Health care providers cannot invite or allow media personnel, including film crews, into treatment or other areas of their facilities where patients' PHI will be accessible in written, electronic, oral, or other visual or audio form, or otherwise make PHI accessible to the media, without prior written authorization from each individual who is or will be in the area or whose PHI otherwise will be accessible to the media."

General Guidelines

- Do not proactively disclose information about a patient to immigration enforcement officials unless a HIPAA law enforcement permission applies. [Crime on premises?]
- Do not invite immigration enforcement officials into treatment areas unless a HIPAA law enforcement permission applies (e.g., court order, court-ordered warrant, patient's HIPAA-compliant authorization).
- HIPAA is unclear on whether you must actively block immigration enforcement officials from entering treatment areas if they insist on doing so.
  - Are you "providing access" if they insist on access and threaten obstruction?
  - Is it ever a "reasonable safeguard" to obstruct an immigration enforcement official from performing their duties?

General Guidelines

- ~~Attestation requirement is causing a lot of friction, so expect push back from immigration enforcement agencies if they request PHI that could encompass reproductive health care information.~~
- Under current administration, OCR is unlikely to allege a HIPAA violation if you cooperate with immigration enforcement officials. State AGs, however, are different stories.
- It is ultimately a risk-based decision – balancing likelihood of HIPAA or AG enforcement vs. risk from immigration enforcement vs. best interests of patients.

AI and Health Data

Davis Wright Tremaine LLP

HIPAA and AI

- AI can be used to support treatment, payment, and health care operations.
- Development of AI:
  - Health care operations? Must be primarily to benefit the covered entity.
  - Research? Must be “systematic investigation” and intended to contribute to generalizable knowledge.
  - Part of delivering a TPO service? Does improving the service fall within providing the service?
  - Proper management and administration of business associate?
  - De-identified data.
- Sale of PHI – Is covered entity providing technology company with access to PHI in exchange for remuneration (discount, free services, IP rights, etc.)?

State Laws

- California Consumer Privacy Act (CCPA)
  - Regulates “profiling” using AI, but does not apply to PHI that is collected by a HIPAA covered entity.
  - Any contract for the sale or license of deidentified information derived from PHI, where one of the parties is a person residing or doing business in California, shall include the following, or substantially similar, provisions:
    1. A statement that the deidentified information being sold or licensed includes deidentified patient information.
    2. A statement that reidentification, and attempted reidentification, of the deidentified information by the purchaser or licensee of the information is prohibited pursuant to this section.
    3. A requirement that, unless otherwise required by law, the purchaser or licensee of the deidentified information may not further disclose the deidentified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions.

State Laws

- Colorado AI Act
  - High-risk AI system includes any AI system that makes or is a substantial factor in making a decision that impacts provision of health care services.
  - A deployer of a high-risk AI system shall:
    - Use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination;
    - Implement a risk management policy and program regarding algorithmic discrimination;
    - Complete an impact assessment;
    - Notify the consumer that deployer has deployed a high-risk AI system, the purpose, and the right to opt out;
    - Provide additional information about adverse consequential decisions; and
    - Website notice.
  - FDA and ONC exemptions.
  - HIPAA exemption if involves health care provider action to implement and not high risk.

Confidentiality of Substance Use Disorder Patient Treatment Records

Davis Wright Tremaine LLP

42 C.F.R. Part 2

- 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 consent 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 pursuant to TPO consent can further use and disclose as permitted under HIPAA [Not clear if limited to general, one-time T,P, *and* O consent or whether applies to more limited T, P, *or* O 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 for Part 2 programs to segregate data, despite tech limitations
  - 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 Health Information Privacy Laws

Davis Wright Tremaine LLP

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)

Reproductive Health Privacy Laws

- California and other states are enacting laws limiting disclosure of reproductive health care (and sometimes gender affirming care).
- Creating potential obstacles to interstate HIE.
- After *Purl* vacated 2024 HIPAA amendments to safeguard reproductive health care privacy, more state laws may be likely.

FTC Enforcement of Health Privacy

Davis Wright Tremaine LLP

FTC Health Information Privacy Enforcement

- Section 5 of the FTC Act – Prohibition on Unfair and Deceptive Practices
  - Basis for FTC's general privacy and security enforcement.
  - Generally, does not apply to non-profits.
  - Has been applied to HIPAA covered entities and business associates.
  - Likely to lessen under new administration.
- FTC Health Breach Notification Rule
  - Applies to personal health records (PHRs), which FTC interprets very broadly.
  - Does not apply to PHI that is subject to HIPAA.
  - FTC less likely to interpret PHR as broadly under new administration.

Questions?

Adam Greene

Partner, Washington, DC
David Wright Tremaine

adamgreene@dwt.com
P: 202.973.4213


Davis Wright
Tremaine LLP