

Health Privacy + Security Law

Fall 2024 Privacy + Security Forum

October 23, 2024

Adam Greene, Partner, Davis Wright Tremaine LLP

Agenda

- Changes to HIPAA
- FTC's Focus on Consumer Health Information
- State Privacy Laws
- Website Disclosures of Personal Information in Healthcare
- Washington My Health My Data Act
- Confidentiality of Substance Use Disorder Patient Records
- Update on Information Blocking Rule
- Q&A



AGENDA

Changes to HIPAA

Overview of Reproductive Health Care Amendments

Prohibition on certain disclosures related to lawful reproductive health care.

Attestation requirement for certain requests.

Revisions to notices of privacy practices.

Additional requirement for law enforcement requests.



The New Prohibition on Use and Disclosure

Scenario #1

- State law bans all abortions except to save life of the pregnant person, or in cases of rape or incest that have been reported to law enforcement.
- Physician performs abortion on pregnant woman who indicated that she was raped but had not reported the rape to law enforcement.
- Hospital receives request from the state attorney general's office for the medical records related to the procedure, accompanied by a warrant.

Scenario #2

- A Texas woman traveled to Colorado to have an abortion, where the procedure was legal.
- Ex-partner seeks to pursue wrongful death claim against anyone involved in the procedure.
- Texas court order requires the Colorado health system to disclose the medical record of the procedure.

The Washington Post

Democracy Dies in Darkness

Texas man files legal action to probe ex-partner's out-of-state abortion

The previously unreported petition reflects a potential new antiabortion strategy to block women from ending their pregnancies in states where abortion is legal.



By [Caroline Kitchener](#)

May 3, 2024 at 5:00 a.m. EDT

As soon as Collin Davis found out his ex-partner was planning to travel to Colorado to have an [abortion](#) in late February, the Texas man retained a high-powered antiabortion attorney — who court records show immediately issued a legal threat.

If the woman proceeded with the abortion, even in a state where the procedure remains legal, Davis would seek a full investigation into the circumstances surrounding the abortion and “pursue wrongful-death claims against anyone involved in the killing of his unborn child,” the lawyer wrote in a letter, according to records.

Now, Davis has disclosed his former partner's abortion to a state district court in Texas, asking for the power to investigate what his lawyer characterizes as potentially illegal activity in a state where almost all abortions are

The New HIPAA Prohibition



Subject to the Rule of Applicability and the Presumption, a covered entity or business associate may not use or disclose PHI for any of the following activities:

1. To conduct a criminal, civil, or administrative investigation (“Investigation”) into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.
2. To impose criminal, civil, or administrative liability (“Liability”) on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.
3. To identify any person for any purpose described above.

Rule of Applicability

The prohibition applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and the covered entity or business associate that received the request for PHI has reasonably determined that one or more of the following conditions exists:

1. The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.
2. The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

Scenario #1

With appropriate attestation (to be discussed), HIPAA will not prohibit the disclosure of PHI, because:

- The reproductive health care was not lawful under the circumstances in which it was provided; and
- Was not protected, required, or authorized by federal law.

State law bans all abortions except to save life of the pregnant person, or in cases of rape or incest that have been reported to law enforcement.

Physician performs abortion on pregnant woman who indicated that she was raped but had not reported the rape to law enforcement.

Hospital receives request from the state attorney general's office for the medical records related to the procedure, accompanied by a warrant.

Scenario #2

HIPAA will prohibit the disclosure of PHI, because:

- The reproductive health care was lawful under the circumstances in which it was provided; and
- The requested disclosure is to impose liability on persons for obtaining, providing, or facilitating reproductive health care.

A Texas woman traveled to Colorado to have an abortion, where the procedure was legal.

Ex-partner seeks to pursue wrongful death claim against anyone involved in the procedure.

Texas court order requires the Colorado health system to disclose the medical record of the procedure.

Scenario #3

- A Nebraska health care provider treats a new patient and downloads a copy of her medical record from a health information exchange.
- The record includes information about an abortion that she received in South Carolina at 7 weeks gestation.
- The Nebraska health care provider receives a court order from a South Carolina court requiring disclosure of the patient's complete medical record.

THE YALE LAW JOURNAL FORUM

OCTOBER 18, 2022

The Abortion Interoperability Trap

Carleen M. Zubrzycki

ABSTRACT. Legislatures in blue states are trying to shield patients' medical records from being used against them in antiabortion litigation and persecutions. The problem is, as medical records increasingly follow the patient, those records are likely to end up in the hands of actors who are not subject to safe-haven laws and who can easily be required to hand over the records to law enforcement or private litigants. Legislatures, policymakers, and private actors should all take steps to close the loopholes that allow this.

INTRODUCTION

There is a serious gap in blue states' efforts to create abortion "safe havens" for the post-*Roe* world. Medical care procured outside a patient's home state increasingly leaves a digital trail that will easily make its way back to the patient's domicile. In the context of abortion—and other controversial forms of healthcare, like gender-affirming treatments—this means that cutting-edge legislative protections for medical records fall short.

In advance of the anticipated fall of *Roe v. Wade*,¹ some state legislatures began to bar in-state medical providers from directly handing over abortion records for use in out-of-state lawsuits or prosecutions in an effort to protect abortion seekers and providers.² After the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*,³ more states are joining the fray.⁴ But these

The Presumption



The reproductive health care provided by another person is presumed lawful under the Rule of Applicability unless the covered entity or business associate has any of the following:

1. Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.
2. Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

Scenario #3

- The Nebraska health care provider, who does not know the law of South Carolina, should presume that the reproductive health care was lawful and should not disclose the requested PHI.
- If the court provides factual evidence, such as an affidavit from someone who witnessed the procedure, demonstrating that the procedure was unlawful, then the provider may disclose the PHI.

A Nebraska health care provider treats a new patient and downloads a copy of her medical record from a health information exchange.

The record includes information about an abortion that she received in South Carolina at 7 weeks gestation.

The Nebraska health care provider receives a court order from a South Carolina court requiring disclosure of the patient's complete medical record.



Attestation Requirements

When an Attestation Is Required

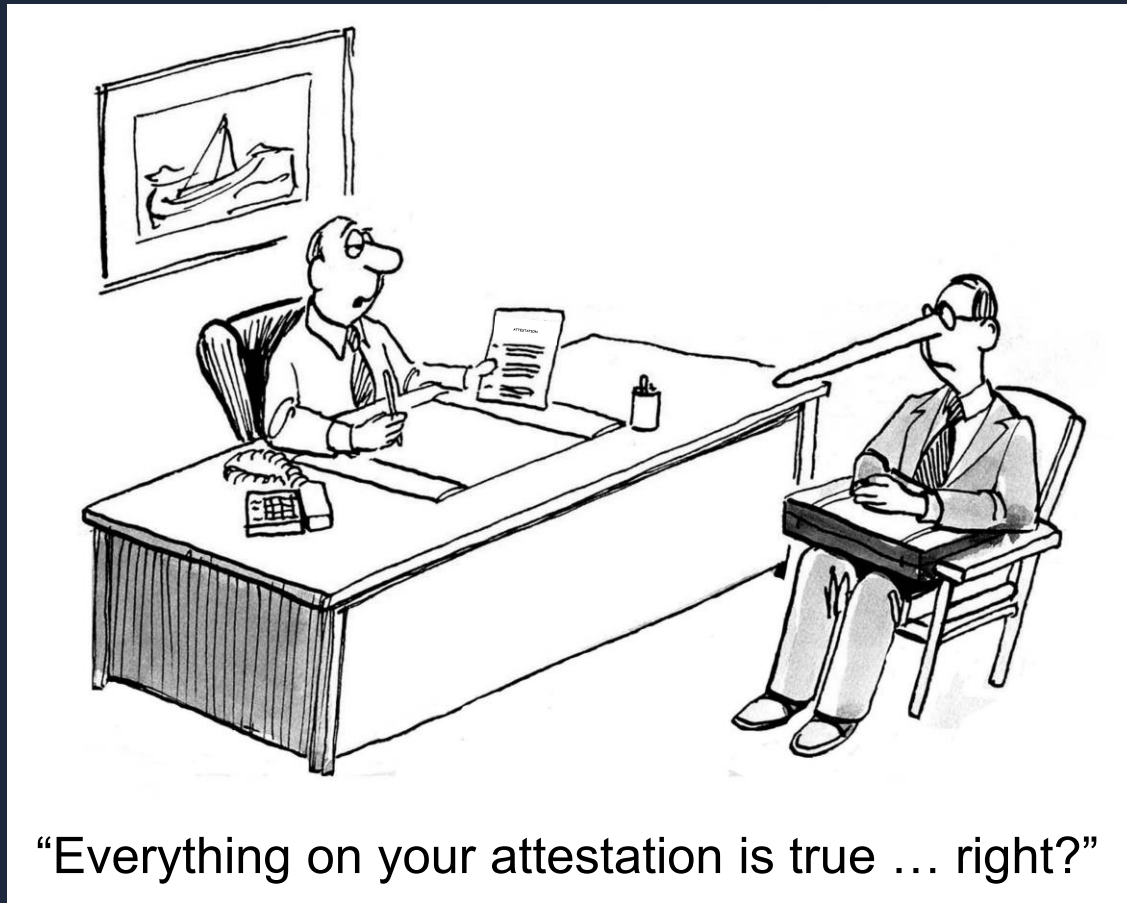
A covered entity or business associate may not use or disclose protected health information potentially related to reproductive health care for the below purposes without obtaining a valid attestation from the person requesting the use or disclosure and complying with all applicable conditions:

- Uses and disclosures for health oversight activities;
- Disclosures for judicial and administrative proceedings;
- Disclosures for law enforcement purposes; or
- Uses and disclosures about decedents — Coroners and medical examiners.

Requirements of an Attestation

- **Description of PHI.** A description of the requested PHI, including:
 - The name of any individual(s) whose PHI is sought, if practicable; or
 - If including the name(s) of any individual(s) whose PHI is sought is not practicable, a description of the class of individuals whose PHI is sought.
- **Disclosing Entity.** The name or class of persons requested to make the use or disclosure.
- **Requestor.** The name or class of persons to whom the covered entity is to make the requested use or disclosure.
- **Not Prohibited.** A clear statement that the use or disclosure is not for a purpose prohibited by the new prohibition.
- **Criminal Penalties.** A statement that a person may be subject to criminal penalties for knowingly and in violation of HIPAA obtaining or disclosing individually identifiable health information.
- **Signature.** Signature of requestor and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.

Defective Attestations



“Everything on your attestation is true ... right?”

- **Too little.** Lacks a required element or statement;
- **Too much.** Includes an additional element of statement;
- **Compound attestation.** Combined with another document;
- **Actual knowledge.** Covered entity or business associate has actual knowledge that material information in the attestation is false; or
- **Unreasonable.** A reasonable covered entity or business associate would not believe the attestation is true with respect to not being for a prohibited purpose.

Scenario #4

- Ohio medical board issues subpoena to an Ohio physician for information about whether the physician performed an abortion out-of-state.
- The physician requests an attestation from the medical board indicating that the request is not to impose liability for providing reproductive health care.
- The board refuses to provide the attestation and threatens to revoke the physician's license for failure to respond.
- HIPAA will not permit the physician to provide the subpoenaed PHI.

Ohio Rev. Code Ann. § 4731.22 provides that the state medical board shall discipline a physician for “commission of an act that constitutes a felony in this state, regardless of the jurisdiction in which the act was committed.”



Revisions to Notices of Privacy Practices

Notice of Privacy Practices

- A description, including at least one example, of the types of uses and disclosures prohibited related to reproductive health care in sufficient detail for an individual to understand the prohibition.
- A description, including at least one example, of the types of uses and disclosures for which an attestation is required.
- A statement about the potential for PHI disclosed pursuant to the Privacy Rule to be redisclosed by the recipient and no longer be protected by the Privacy Rule.
- Information about protections for substance use disorder (SUD) records subject to 42 C.F.R. part 2 (if applicable).
- If covered entity intends to use SUD records subject to 42 C.F.R. part 2 for fundraising, then clear and conspicuous opportunity to opt out.
- Other minor changes related to 42 C.F.R. part 2 (where applicable).



Additional Requirement for Law Enforcement Requests

Law Enforcement Administrative Requests

A covered entity may disclose protected health information: ...

(ii) In compliance with and as limited by the relevant requirements of: ...

(C) An administrative request for which response is required by law, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

1. The information sought is relevant and material to a legitimate law enforcement inquiry;
2. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
3. De-identified information could not reasonably be used.

Law Enforcement Administrative Requests

- Applies to any law enforcement administrative request (not just related to reproductive health care)
- HHS indicated that this was always intent and does not represent a substantive change.
- If written law enforcement request includes required elements, when is it obstruction of justice to not respond?





Other Miscellaneous Changes

Other Miscellaneous Changes

- *Person* means a natural person (meaning a human being who is born alive), trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- *Public health*, as used in the terms “public health surveillance,” “public health investigation,” and “public health intervention,” means population-level activities to prevent disease in and promote the health of populations. Such activities include identifying, monitoring, preventing, or mitigating ongoing or prospective threats to the health or safety of a population, which may involve the collection of protected health information. But such activities do not include those with any of the following purposes:
 1. To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating health care.
 2. To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating health care.
 3. To identify any person for any of the activities described at paragraphs (1) or (2) of this definition.

Other Miscellaneous Changes

- *Reproductive health care* means health care, as defined in this section, that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care.
- Revisions to: (1) exemption for personal representative in cases of abuse, neglect, endangerment situations; and (2) disclosures about victims of abuse, neglect, or domestic violence; clarifying that provision or facilitation of reproductive health care is not abuse, neglect, or domestic violence.



Next Steps and Challenges Ahead

Next Steps

- Revise policies and procedures to implement prohibition and attestation requirement.
- Train release of information department on limiting disclosures and obtaining attestations.
- Revise notice of privacy practices.
- Compliance deadlines are:
 - December 23, 2024 (Merry Christmas), except
 - February 16, 2026 for changes to notice of privacy practices.



Challenges Ahead

- Identifying when PHI may potentially relate to reproductive health care.
 - Some business associates may not have visibility into nature of PHI.
- Refusing or challenging government requests that are contrary to prohibition or do not include attestation.
- Determining when it is unreasonable to believe an attestation.



UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
LUBBOCK DIVISION

VII. DEMAND FOR RELIEF

Texas respectfully requests that the Court:

- a. Declare that the 2000 Privacy Rule and the 2024 Privacy Rule violate the Administrative Procedure Act because they exceed statutory authority;
- b. Declare that the 2000 Privacy Rule and the 2024 Privacy Rule violate the Administrative Procedure Act because they are arbitrary and capricious;
- c. Vacate and set aside the 2000 Privacy Rule and the 2024 Privacy Rule and permanently enjoin Defendants from enforcing them;
- d. Grant Texas an award of attorneys' fees and other litigation costs reasonably incurred in this action; and
- e. Grant Texas such other relief as the Court deems just and proper and as justice so requires.

effective in 2001. This lawsuit challenges the portion of the 2000 Privacy Rule that purports to limit disclosures to State investigators (45 C.F.R. § 164.512(f)(1)(ii)(C)).

3. The second is entitled "HIPAA Privacy Rule to Support Reproductive Health Care Privacy," 89 Fed. Reg. 32,976 (April 26, 2024) (the "2024 Privacy Rule") and became effective on June 25, 2024.

Changes to the Security Rule

- “This rule will propose modifications to the [Security Rule] under [HIPAA] and the [HITECH Act]. These modifications will improve cybersecurity in the health care sector by strengthening requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats.”
- Timetable: December 2024 (aspirational)

10/14/24, 3:36 PM View Rule

An official website of the United States government

OFFICE of INFORMATION and REGULATORY AFFAIRS
OFFICE of MANAGEMENT and BUDGET
EXECUTIVE OFFICE of the PRESIDENT

Reginfo.gov

U.S. General Services Administration GSA

Search: Agenda Reg Review ICR

Home Unified Agenda Regulatory Review Information Collection Review FAQs / Resources Contact Us

View Rule

[View EO 12866 Meetings](#) [Printer-Friendly Version](#) [Download RIN Data in XML](#)

HHS/OCR RIN: 0945-AA22 Publication ID: Spring 2024

Title: Proposed Modifications to the HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information

Abstract:
This rule will propose modifications to the Security Standards for the Protection of Electronic Protected Health Information (the 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). These modifications will improve cybersecurity in the health care sector by strengthening requirements for HIPAA regulated entities to safeguard electronic protected health information to prevent, detect, contain, mitigate, and recover from cybersecurity threats.

Agency: Department of Health and Human Services(HHS) **Priority:** Section 3(f)(1) Significant
RIN Status: Previously published in the Unified Agenda **Agenda Stage of Rulemaking:** Proposed Rule Stage
Major: Yes **Unfunded Mandates:** Undetermined

CFR Citation: [45 CFR 160](#) [45 CFR 164](#)

Legal Authority: [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\), sec. 262 \(42 U.S.C. 1320d-2\)](#) [Health Information Technology for Economic and Clinical Health \(HITECH\) Act, sec. 13401 \(42 U.S.C. 17931\)](#)

Legal Deadline: None

Timetable:

Action	Date	FR Cite
NPRM	12/00/2024	

Regulatory Flexibility Analysis Required: Undetermined **Government Levels Affected:** Undetermined
Small Entities Affected: Businesses, Governmental Jurisdictions, Organizations **Federalism:** Undetermined

Included in the Regulatory Plan: Yes

International Impacts: This regulatory action will be likely to have international trade and investment effects, or otherwise be of international interest.

RIN Data Printed in the FR: No

Agency Contact:
Marissa Gordon-Nguyen
Senior Advisor for Health Information Privacy, Data, and Cybersecurity Policy
Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue SW,
Washington, DC 20201
Phone:800 368-1019
TDD Phone:800 537-7697
Email: ocrprivacy@hhs.gov

Give Feedback

Other Changes to HIPAA

Rule	Last Action	Next Action
2021 Coordinated Care NPRM	NPRM published 1/21/21, comment period ended 5/6/21	Final rule (2025?)
April 2022 RFI on Distribution of Penalties and Recognized Security Practices	Comments due 6/6/22	NPRM (?)

FTC Focus on Consumer Health Information

Recent Enforcement Actions

GoodRx (2/1/23)



- Disclosure of website data to third parties advertising platforms
- Section 5 + HBNR
- \$1.5 million civil monetary penalty

BetterHelp (3/2/23)



- Disclosure of website data to third parties advertising platforms
- Section 5
- \$7.8 payment to consumers

Premom (5/17/23)



- Disclosure of website data to third parties advertising platforms
- Section 5 + HBNR
- \$100,000 civil monetary penalty

1Health.io (6/16/23)



- Failure to destroy samples, failure to get opt in to change in privacy policy, lack of security
- Section 5
- \$75,000 payment for consumer refunds

Recent Enforcement Actions

Monument (4/11/24)



- Disclosure of website data to third parties advertising platforms
- Section 5 + Opioid Addiction Recovery Fraud Prevention Act
- \$2.5M civil monetary penalty

Cerebral (4/15/24)



- Disclosure of website data to third parties advertising platforms
- Section 5 + Opioid Addiction Recovery Fraud Prevention Act
- \$15M civil monetary penalty (\$8M suspended)

Health Breach Notification Rule (HBNR)

- Conforms regulations to September 2021 Policy Statement
- Applies HBNR to broad range of health and wellness apps
- Clarifies that “breach of security” includes any use or disclosure not authorized by consumer
- Provides more time to notify FTC

Billing Code: 6750-01P

FEDERAL TRADE COMMISSION

16 CFR Part 318

RIN 3084-AB56

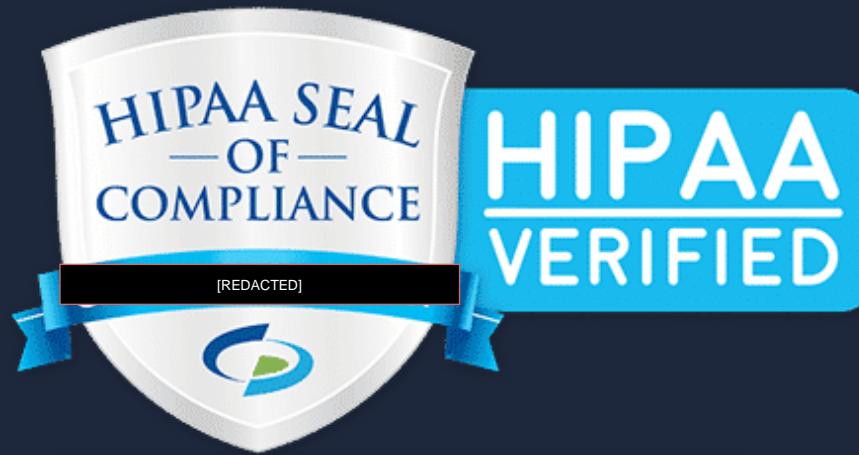
Health Breach Notification Rule

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission (“FTC” or “Commission”) is amending the Commission’s Health Breach Notification Rule (the “HBN Rule” or the “Rule”). The HBN Rule requires vendors of personal health records (“PHRs”) and related entities that are not covered by the Health Insurance Portability and Accountability Act (“HIPAA”) to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. The amendments: (1) clarify the Rule’s scope, including its coverage of developers of many health applications (“apps”); (2) clarify what it means for a vendor of personal health records to draw PHR identifiable health information from multiple sources; (3) revise the definition of

Same Statute, Different Interpretations?



State Privacy laws

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

* Does not include thresholds based on % of revenue from sale of personal data.

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

* Does not include thresholds based on % of revenue from sale of personal data.

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

* Does not include thresholds based on % of revenue from sale of personal data.

New York Cybersecurity Requirements (Oct. 2, 2024)

- Applies to NY general hospitals.
- Requires notification to NY Department of Health within 72 hours after determining a cybersecurity incident has occurred.
- More detailing information security requirements than HIPAA Security Rule



Website Disclosures of Personal Information in Healthcare

I'm looking for...

[A-Z Index](#)HIPAA for
IndividualsFiling a
ComplaintHIPAA 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](#)

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 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

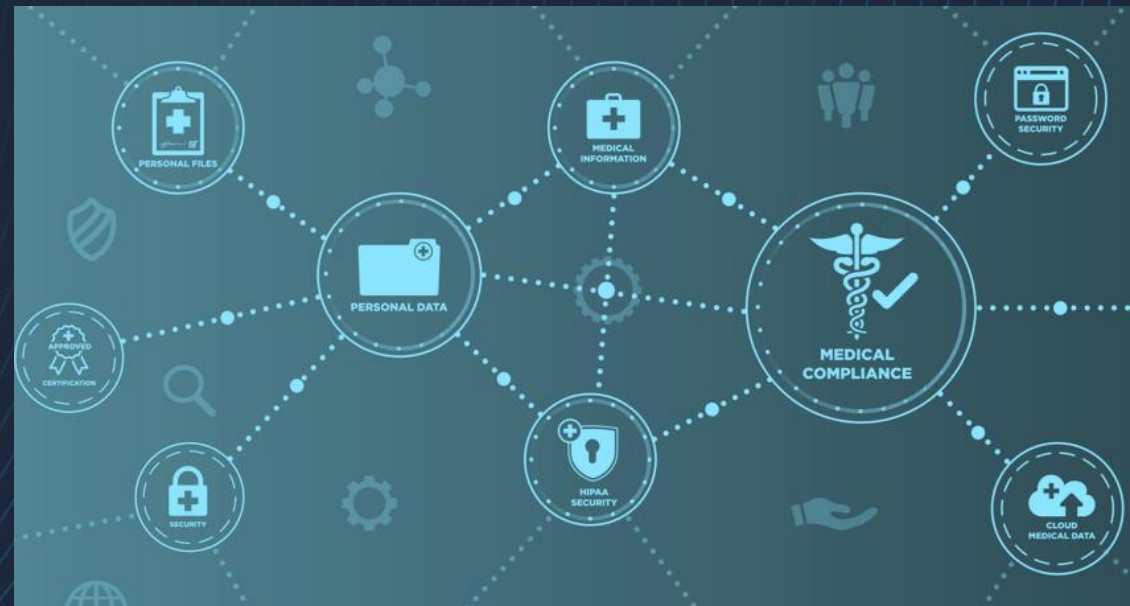
Websites and PHI



- Is website tracking information individually identifiable?
 - Email address
 - IP address
 - Unique identifier in cookie or login

Websites and PHI

- Is website tracking information Health Information?
 - According to guidance, yes if:
 - Authenticated page limited to patients/members
 - Unauthenticated page but reveals:
 - Login
 - Scheduling an appointment
 - Search for a doctor
 - Specific condition or treatment
 - According to guidance, no if only identifies that someone visited home page/non-condition specific page and does not reveal health-related actions



OCR and FTC Send Joint Letter to ~ 130 Health Care Providers



July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,¹ news reports,² FTC enforcement actions,³ and an OCR bulletin⁴ have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

FTC Publishes Blog on Website Health Info Privacy

[Home](#) / [Business Guidance](#) / [Business Blog](#)

Business Blog

Protecting the privacy of health information: A baker's dozen takeaways from FTC cases

By: [Elisa Jillson](#) | July 25, 2023 | [f](#) [t](#) [in](#)

In the past few months, the FTC has announced case after case involving consumers' sensitive health data, alleging violations of both Section 5 of the FTC Act and the FTC's [Health Breach Notification Rule](#). The privacy of health information is top of mind for consumers – and so it's top of mind for the FTC. Companies collecting or using health data, listen up. There are a number of key messages from [BetterHelp](#), [GoodRx](#), [Premom](#), [Vitagene](#), and other FTC matters that you need to hear.

Get Business Blog updates


Topics

[Advertising and Marketing \(523\)](#)

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


2/5/24, 10:23 AM Hospital associations and hospitals file lawsuit challenging federal rule that ties providers' hands in efforts to reach communities | ...

 American Hospital Association

News (taxonomy/term/104) / Headline (taxonomy/term/107)

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.aha.org/legal-documents/2023-11-02-case-complaint-aha-the-united-health-care-system-v-rainier> the federal government to bar enforcement of an unlawful, harmful and counterproductive rule that has upended 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.aha.org/news/headline/2023-11-02-hospital-associations-and-hospitals-file-lawsuit-challenging-federal-rule-ties-providers-hands-efforts> 1/5

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) ≠ IHI (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.”



Washington
My Health
My Data Act

Washington My Health My Data Act

- Covers “consumer health data” (CHD), which is broadly defined but excludes PHI.
- Covers WA residents and non-WA residents whose information is bought, rented, accessed, retained, received, acquired, inferred, derived, or otherwise processed in WA.
- Private right of action but must prove damages.

Washington My Health My Data Act

- **Transparency.** Posting of consumer health data privacy policy.
- **Consent.** Obtain consent to collect or share CHD (other than as necessary to provide product or service).
- **Authorization for Sale.** More detailed authorization for sale of CHD, including name and contact info of purchasers.
- **Geofencing Restriction.** Restrict on geofencing around health care entities.

Washington My Health My Data Act

- Consumer Rights.
 - Confirmation of collection, sharing, or selling CHD.
 - Access to CHD and list of third parties and affiliated with whom CHD was shared or sold.
 - Right to withdraw consent.
 - Right of deletion.
- Security Obligations. Reasonable security practices to protect confidentiality, integrity, and accessibility.

Washington AG FAQs

Is a business that is covered by the My Health My Data Act required to place a link to its Consumer Health Data Privacy Policy on the company's homepage?

Yes. Section 4(1)(b) of the My Health My Data Act explicitly provides that “[a] regulated entity and a small business shall prominently publish a link to its consumer health data privacy policy on its homepage.” The Consumer Health Privacy Policy must be a separate and distinct link on the regulated entity's homepage and may not contain additional information not required under the My Health My Data Act.

Washington AG FAQs

Does the definition of consumer health data include the purchase of toiletry products (such as deodorant, mouthwash, and toilet paper) as these products relate to “bodily functions”?

Information that does not identify a consumer’s past, present, or future physical or mental health status does not fall within the Act’s definition of consumer health data. Ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data. For example, while information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone’s digestion or perspiration is collecting consumer health data.

Washington AG FAQs

Does the definition of consumer health data include the purchase of non-prescription medication?

MHMD defines consumer health data to include the “use and purchase of prescribed medication.” Non-prescription data is only considered consumer health data if the regulated entity draws an inference about a consumer’s health status from its purchase of non-prescription medication.



Challenges

- Consent for collection of CHD.
- Ambiguity over scope of CHD.
- No exceptions to right of deletion.
- Listing of all third parties to whom disclosures of CHD are made.
- Separate consumer health data privacy policy.



Confidentiality of Substance Use Disorder Patient 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.
 - Quality 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)

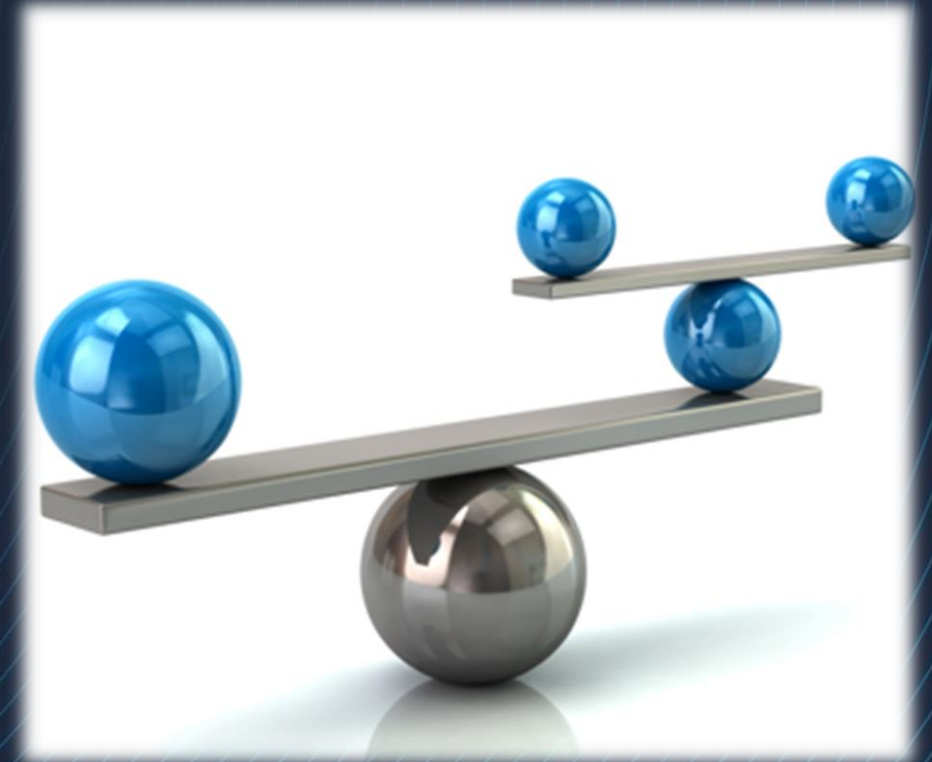


- Likely impact:
 - Continued need to segregate data
 - Increased risk of enforcement
- Remaining question: If patient provides limited consent, can CE/BA recipient use and disclose to the extent permitted by HIPAA?
- Compliance date: February 16, 2026

Update on Information Blocking

Cures Act – Information Blocking Definition

- Except if:
 - Practice is required by law
 - Falls under HHS rulemaking exception
- Practice is likely to ...
- Interfere with, prevent, or materially discourage ...



Cures Act – Information Blocking Definition (Cont'd)

- Access, exchange, or use ...
- Electronic Health Information
- Knowledge
 - Knows or Should Know (health information technology developer, exchange, or network); or
 - Knows practice is unreasonable (health care provider)

Information Blocking - Actors



Health Care Providers



Health IT Developers of
Certified Health IT



Health Information
Networks/Health
Information Exchanges

Eight-Nine Exceptions



HHS Office of the National Coordinator of Health IT, <https://www.healthit.gov/topic/information-blocking>

Recent Changes (January 2024)

- Defined “offer health IT” for purposes of definition of a health IT developer.
 - To hold out for sale, resale, license, or relicense or to sell, resell, license, relicense, or otherwise provide or supply health information technology which includes one or more certified Health IT Modules for deployment by or for other individual(s) or entity(ies) under any arrangement.
- Correspondingly revised definition of health IT developer.

Recent Changes (January 2024)

- “Offering health IT” does not include:
 - **Funding.** Does not cover provides funds to cover health care provider’s acquisition, augmentation, or upkeep of health if not tied to inappropriate limitations.
 - **Certain Implementation and Use Activities.** E.g., issuing user accounts or login credentials, implementing an API or patient portal, etc.
 - **Certain Consulting and legal services.** E.g., certain outside counsel, consulting, or non-health IT administrative services related to acquiring or implementing health IT.

Recent Changes (January 2024)

- Removes limitations of scope of EHI that expired in October 2022 (i.e., the USCDI) from definition of information blocking and content and manner exception (now simply the “manner exception”)
- Infeasibility Exception
 - Clarify that infeasibility must be “because of” an uncontrollable event that “in fact negatively impacts the actor’s ability to fulfill the request.”
 - Exemption from having to allow a third party to modify EHI.
 - Exemption if actor cannot reach agreement or technically fulfill request after offering at least two alternative manners from Manner Exception and does not offer the requested access to a substantial number of others.

Recent Changes (January 2024)

- Trusted Exchange Framework and Common Agreement (TEFCA)
 - New subpart in exceptions devoted to TEFCA
 - If requestor can access the EHI through TEFCA, then actor does not need to provide alternative manner.
 - To satisfy the exception:
 - Both actor and requestor are part of TEFCA
 - Requestor is capable of access, exchange, or use of requested EHI through TEFCA
 - Request is not via API standards adopted under EHR certification standards
 - Any fees and license requirements satisfy Fees and Licensing Exceptions

Information Blocking Penalties

- Civil monetary penalties up to \$1 million per violation for:
 - Health IT developers of certified health IT
 - HIEs/HINs
- Health care providers → “appropriate disincentives” that fall under existing authority – awaiting rulemaking



Status of Enforcement

Health IT Developers and HIEs/HINs

- Applicability date was April 5, 2021
- OIG enforcement with respect to health IT developers and HIEs/HINs:
 - \$1 million per violation
 - Final enforcement rule on July 3, 2023
 - Enforcement rule became effective September 1, 2023

Status of Enforcement Health Care Providers



- Enforcement with respect to health care providers:
 - Final rule's effective date was July 31, 2024.
 - Lower Medicare reimbursement due to not qualifying as a “meaningful user of certified EHR technology” under Promoting Interoperability Program (eligible hospitals and critical access hospitals) and MIPS program (eligible professionals).
 - Potential exclusion from Medicare Shared Savings Program for one year.
 - No disincentives outside of Medicare program.
 - OIG investigates and refers to CMS.

Proposed Changes (August 2024)

(Comments due 10/4/24)

Proposed examples of “interferences”

1. *Delay on new access.* Delaying patient access to new EHI, such as diagnostic testing results, so clinicians or other actor representatives can review the EHI.
2. *Portal access.* Delaying patient access to EHI in a portal when the actor has the EHI and the actor's system has the technical capability to support automated access, exchange, or use of the EHI via the portal.
3. *API access.* Delaying the access, exchange, or use of EHI to or by a third-party app designated and authorized by the patient, when there is a deployed application programming interface (API) able to support the access, exchange, or use of the EHI.



Proposed Changes (August 2024)

(Comments due 10/4/24)

Proposed examples of “interferences” (cont’d)

4. *Non-standard implementation.* Implementing health information technology in ways that are likely to restrict access, exchange, or use of EHI with respect to exporting electronic health information, including, but not limited to, exports for transitioning between health IT systems.
5. *Contract provisions.* Negotiating or enforcing a contract provision that restricts or limits otherwise lawful access, exchange, or use of EHI.
6. *Non-compete provisions in agreements.* Negotiating or enforcing a clause in any agreement that:
 - i. Prevents or restricts an employee (other than the actor's employees), a contractor, or a contractor's employee ...
 - ii. Who accesses, exchanges, or uses the EHI in the actor's health IT ...
 - iii. From accessing, exchanging, or using EHI in other health IT in order to design, develop, or upgrade such other health IT.

Proposed Changes (August 2024)

(Comments due 10/4/24)



Proposed examples of “interferences”

7. *Manner or content requested.* Improperly encouraging or inducing requestors to limit the scope, manner, or timing of EHI requested for access, exchange, or use.
8. *Medical images.* Requiring that the access, exchange, or use of any medical images (including, but not limited to, photograph, x-rays, and imaging scans) occur by exchanging physical copies or copies on physical media (such as thumb drive or DVD) when the actor and the requestor possess the technical capability to access, exchange, or use the images through fully electronic means.

Proposed Changes (August 2024)

(Comments due 10/4/24)



Proposed examples of “interferences”

9. *Omissions.* The following omissions:
 - i. Not exchanging EHI under circumstances in which such exchange is lawful;
 - ii. Not making EHI available for lawful use;
 - iii. Not complying with another valid law enforceable against the actor that requires access, exchange or use of EHI;
 - iv. A Certified API Developer (as defined in [45 CFR 170.404](#)) failing to publish API discovery details as required by the maintenance of certification requirement in [45 CFR 170.404\(b\)\(2\)](#);
 - v. An API Information Source (as defined in [45 CFR 170.404](#)) failing to disclose to the Certified API Developer the information necessary for the Certified API Developer to publish the API discovery details required by [45 CFR 170.404\(b\)\(2\)](#).

Proposed Changes (August 2024)

(Comments due 10/4/24)

- Reproductive Health Care Access – Not information blocking if practice is implemented to reduce potential exposure to legal action and:
 - Practice is undertaken based on the actor's good faith belief that:
 1. Persons seeking, obtaining, providing, or facilitating reproductive health care are at risk of being potentially exposed to legal action that could arise as a consequence of particular access, exchange, or use of specific electronic health information; and
 2. Specific practices likely to interfere with such access, exchange, or use of such electronic health information could reduce that risk.
 - Practice is no broader than necessary to reduce the risk.
 - Practice is implemented either consistent with an organizational policy that meets certain criteria (e.g., non-discriminatory) or pursuant to a case-by-case determination that meets certain criteria.

Proposed Changes (August 2024)

(Comments due 10/4/24)

- Reproductive Health Care Access
 - Patient Protection Conditions
 - Limited to EHI that could expose the patient to legal action.
 - Patient can require access, exchange, or use of the EHI despite legal risk.
 - Care Access Conditions
 - Limited to EHI that could expose the provider or facilitator to legal action.



Proposed Changes (August 2024)

(Comments due 10/4/24)

- Requestor Preferences Exception

- It is not information blocking to tailor access, exchange, or use of EHI to a requestor's preference if:
 - Requestor requests in writing, without improper encouragement, that the actor:
 - Limit the scope of EHI made available for access, exchange, or use by the requestor;
 - Delay provision of access, exchange, or use by the requestor of particular EHI until a condition specified by the requestor (such as passage of a particular event or completion of an action) has been met; or
 - Delay provision of access, exchange, or use by the requestor of particular EHI for a specified period of time.
 - Practice must be tailored to the specific request and implemented in consistent and non-discriminatory manner.



Questions



For more information ...



Adam Greene

Partner, Washington, DC

Davis Wright Tremaine

adamgreene@dwt.com

P: 202.973.4213