

HIPAA Reproductive Health Rule and Other Health Info Issues



IdHIMA
Idaho HIMSS
Human Tech Idaho
Conference

Kim C. Stanger

(4/25)

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Overview

- Parental Access to Minor's Records
- Reproductive Health Rule
- Proposed HIPAA Rules
 - Privacy
 - Security
- SUD Records
- FTCA Enforcement
- Information Blocking Rule
- AI in Healthcare



Parent's Right to Access Minor's Records



Confidentiality of Minor Records (before 7/1/24)

HIPAA

- If minor may consent to their own healthcare under state law, then...
 - Parent is not “personal representative.”
 - Parent has no right to access info.
 - Generally, need minor’s consent or authorization to disclose.
 - May deny access to avert serious threat of harm.

(45 CFR 164.502(g))

OTHER LAWS

- If minor aged 16+ seeks drug treatment or rehab, may not disclose to parent without minor’s consent. (IC 37-3102)
- If minor seeks care for substance use disorder, may not disclose the request for care to parents. (42 CFR 2.14(b)(2))
- If minor seeks family planning services under Title X, may not disclose to parents. (42 CFR 59.10(b))
- Others?

Parent's Rights in Medical Decision-Making Act

Effective July 1, 2024:

- Must obtain parental consent to treat unemancipated minor with limited exceptions.
- Must allow parents to access unemancipated minor's records with limited exceptions.
- Parents may sue provider for violations and recover damages, costs and attorneys' fees.

(IC 32-1015)

Parental Access to Minor's Records

- “No health care provider or governmental entity shall deny a minor child’s parent access to health information that is ... in such health care provider’s ... control.”
 - "Health info" = info or data, collected or recorded in any form or medium, and personal facts about events or relationships that relates to:
 - (i) Past, present, or future physical, mental, or behavioral health or condition of individual or member of individual’s family;
 - (ii) Provision of health care services to an individual; or
 - (iii) Payment for the provision of health care services to an individual.
- Violation: parent may sue for damages, costs and fees.
(IC 32-1015)
- ✓ *Likely applies to records created or info relating to treatment before 7/1/24.*

Parent's Rights Act: Effect on Prior State Laws?

- IC 32-1015: “This section shall be construed in favor of a broad protection of parents’ fundamental right to make decisions concerning the furnishing of health care services to minor children.” (IC 32-1015(7))
- SB1329 Statement of Purpose: “[C]onsent for the furnishing of health care services to any person who is an unemancipated minor must be given or refused by the parent of such person.... [T]he Act is intended to supersede any current provisions of Idaho law that may otherwise conflict with the Act.” (<https://legislature.idaho.gov/wp-content/uploads/sessioninfo/2024/legislation/S1329SOP.pdf>)
- Idaho courts often look to Statement of Purpose to determine legislative intent. (*Farmers Nat’l Bank v. Green River Dairy, LLC*, 155 Idaho 853, 860 at n.4 (2014))
- General principle: if there is conflict, later law preempts earlier conflicting law v. specific law preempts conflicting general law.
- ✓ *Conservative approach: assume parental consent is needed unless exception applies or we receive further authoritative guidance.*

Parent's Access to Minor's Records: Exceptions

May deny parent access if:

- “Minor is emancipated,” e.g.,
 - Married
 - Serving in active military
 - Self-dependent and rejected parent/child relationship
 - Court declares them emancipated

(See IC 32-1015(5))

- “Parent's access to the requested health info is prohibited by a court order”; or
- “The parent is a subject of an investigation related to a crime committed against the child, and a law enforcement officer requests that the information not be released to the parent.”

(IC 32-1015(6))

Parent's Access to Minor's Records: Federal Preemption?

If a federal law preempts Idaho law and prohibits disclosure, e.g.,

- HIPAA? (45 CFR 164.502(g))
- Substance use disorder programs?
 - “Where state law requires parental consent to treatment, the fact of a minor's application for treatment may be communicated to the minor's parent, guardian, or other person authorized under state law to act on the minor's behalf only if: (i) The minor has given written consent to the disclosure ...; or (ii) The minor lacks the capacity to make a rational choice regarding such consent ...” (42 CFR 2.14(b)(2))
- Title X programs?
 - “Title X projects may not require consent of parents or guardians for the provision of services to minors, nor can any Title X project staff notify a parent or guardian before or after a minor has requested and/or received Title X family planning services.” (42 CFR 59.10(b)).
 - *But see Deandra v. Becerra*, No. 23-10159 (5th Cir. 2024) (holding that Title X regs do not preempt Texas parental consent laws).
- Others?

HIPAA: Preemption

- HIPAA preempts contrary state law unless the state law is more stringent.
(45 CFR 160.203)
- “*More stringent* means, in the context of a comparison of a provision of State law and a standard ... adopted under [the HIPAA privacy rule], a State law that meets one or more of the following criteria:

...

(6)provides greater privacy protection for the individual who is the subject of the individually identifiable health information”

(45 CFR 160.202)

HIPAA: Disclosures to Personal Reps

- Under HIPAA, must treat personal rep as the patient.
 - Personal rep has right to access PHI.
 - “Personal rep” = person with authority to consent to care of patient under state law.
- Exception:
 - “Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal rep ... if:
 - (i) The covered entity has a reasonable belief that:
 - (A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or
 - (B) Treating such person as the personal rep could endanger the individual; and
 - (ii) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual’s personal rep.”

(45 CFR 164.502(g))

HIPAA:

Disclosures to Personal Reps

- “If ... by an applicable provision of State or other law ... a covered entity may disclose, or provide access in accordance with [45 C.F.R.] § 164.524 to, protected health info about an unemancipated minor to a parent, guardian, or other person acting in loco parentis....”

(45 CFR 164.502(g)(3)(ii)(A))

- Under 164.524, may deny patient and personal rep access under certain circumstances, e.g.,
 - PHI outside designated record set.
 - Psychotherapy notes.
 - PHI obtained under promise of confidentiality and disclosure would reveal source of info.
 - Licensed provider determines that disclosure is “reasonably likely to endanger the life or physical safety of the individual or other person”, subject to review.

(45 CFR 164.524)

Non-Custodial Parent Access

- “Notwithstanding any other provisions of law, access to records and information pertaining to a minor child including, but not limited to, medical, dental, health, and school or educational records, shall not be denied to a parent because the parent is not the child’s custodial parent.
- “[I]nformation concerning the minor child’s address shall be deleted from such records to a parent, if the custodial parent has advised the records custodian in writing to do so.”

(IC 32-717A)

HIPAA Reproductive Health Rule

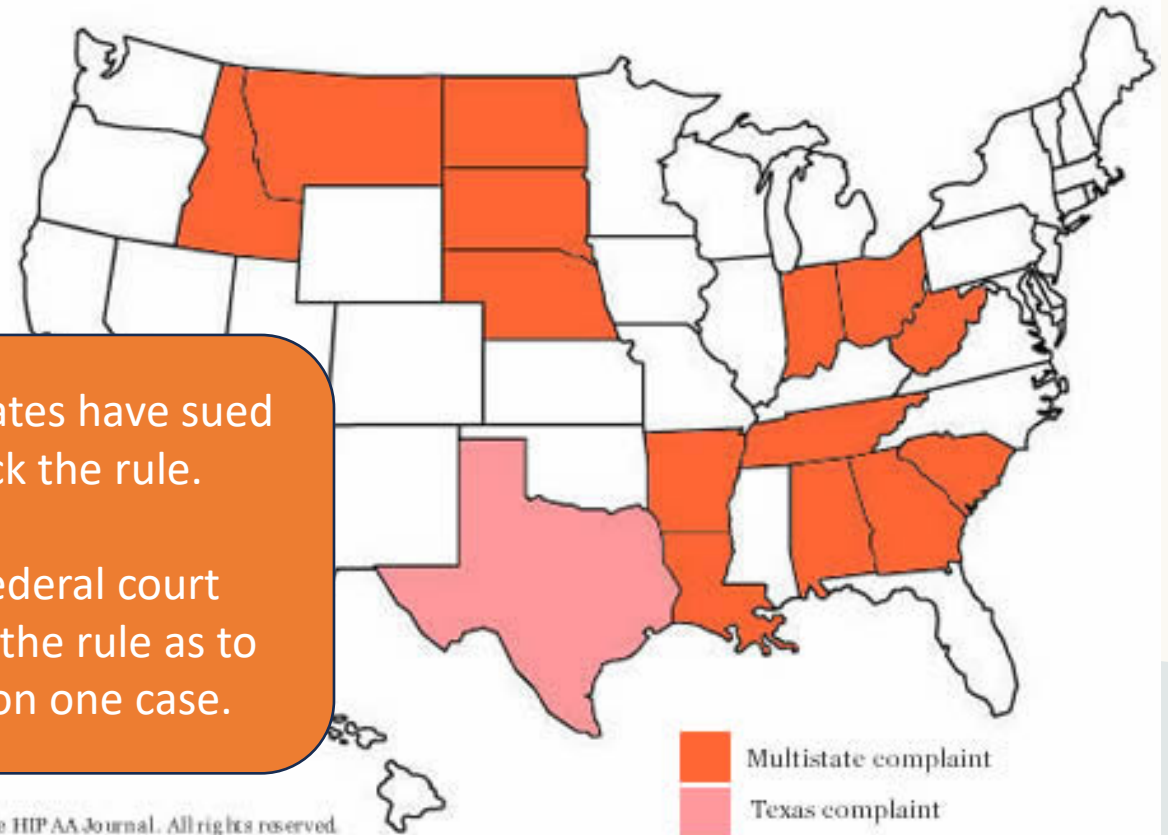


Status of Rule is Uncertain



Trump administration actions suggest it may not push reproductive rights on a federal level.

States Challenging HIPAA Reproductive Healthcare Privacy Final Rule



Several states have sued to block the rule.

Texas federal court enjoined the rule as to parties on one case.

In the meantime, the rule is still on the books and OCR website

Health Information Privacy

<https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/index.html>



HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Special Topics](#) > HIPAA and Reproductive Health

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics -

HIPAA and Part 2

Change Healthcare Cybersecurity Incident FAQs

HIPAA and COVID-19



HIPAA and Reproductive Health

Final Rule HIPAA Privacy Rule to Support Reproductive Health Care Privacy

On April 22, 2024, OCR issued a Final Rule, entitled *HIPAA Privacy Rule to Support Reproductive Health Care Privacy*. The Final Rule strengthens the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by prohibiting the disclosure of protected health information related to lawful reproductive health care in certain circumstances. HHS issued this Final Rule after hearing from communities that changes were needed to better protect patient confidentiality and prevent medical records from

[Back to top](#)

OCR has signaled enforcement in the past

Podcasts

Media Guidelines for HHS Employees

FOR IMMEDIATE RELEASE
November 26, 2024

Contact: HHS Press Office

202-690-6343

media@hhs.gov

- Hospital's disclosure of PHI to patient's employer exceeded patient's authorization.
- Hospital pays \$35,581 and enters corrective action plan.

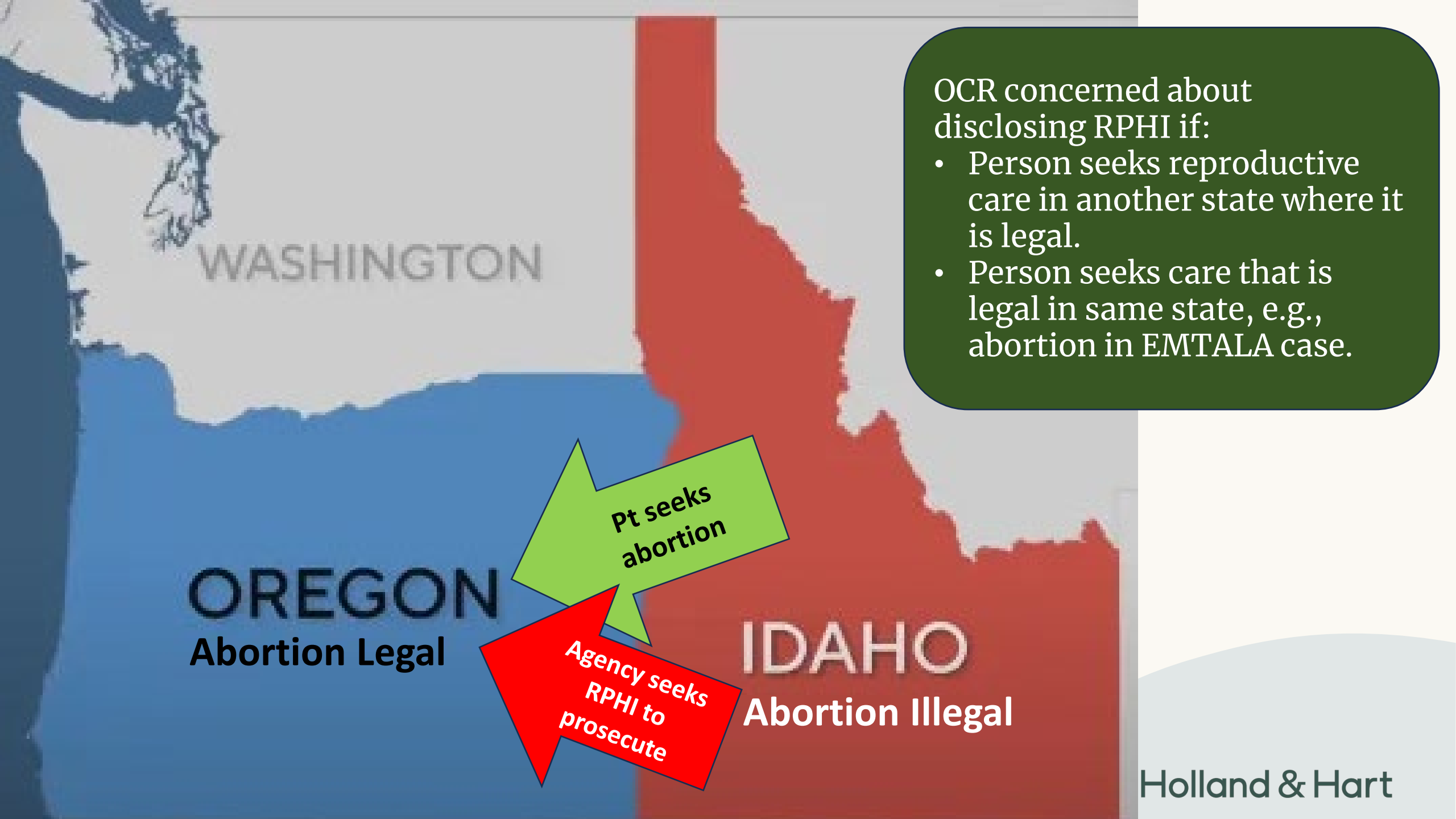
HHS Office for Civil Rights Settles with Holy Redeemer Hospital Over Disclosure of Patient's Protected Health Information, Including Reproductive Health Information

Settlement emphasizes the need to ensure the privacy of PHI, including reproductive health information

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a settlement with Holy Redeemer Family Medicine (Holy Redeemer), a Pennsylvania hospital, concerning an alleged violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule due to an impermissible disclosure of a female patient's protected health information, including information related to reproductive health care. OCR enforces the [HIPAA Privacy, Security, and Breach Notification Rules](#), which set forth the requirements that covered entities (health plans, health care clearinghouses, and most health care providers) and business associates must follow relating to the privacy and security of protected health information. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records, requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization, (such as disclosures for health oversight activities or for law enforcement purposes), and gives individuals rights such as the ability to access their own medical records.

OCR is sending a message:

“OCR is committed to ensuring the privacy of lawful reproductive health care....”



WASHINGTON

OREGON

Abortion Legal

**Pt seeks
abortion**

**Agency seeks
RPHI to
prosecute**

IDAHO

Abortion Illegal

- OCR concerned about disclosing RPHI if:
- Person seeks reproductive care in another state where it is legal.
 - Person seeks care that is legal in same state, e.g., abortion in EMTALA case.

Reproductive Health Rule

Effective 12/23/24:

- If reproductive healthcare was legal, covered entities and business associates may not use or disclose protected health info re reproductive healthcare (“RPHI”) for purposes of criminal, civil or administrative liability or investigation.

(45 CFR 164.502(a)(5))

- Must obtain attestation from persons seeking RPHI for purposes of criminal, civil or administrative investigation or liability to confirm purpose and legality.

(45 CFR 164.509)

- ✓ Ability to use or disclose RPHI depends on—
 - ✓ Legality of the care rendered, and
 - ✓ Purpose for which info is sought,
not necessarily its status as RPHI.

Reproductive Health Care Info ("RPHI")

- Applies to protected health info re "reproductive health care", i.e., "health care that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes."

(45 CFR 160.103)

- Broader than just abortion; extends to any PHI re any reproductive health care ("RPHI").
- Applies to any provider or business associate who has RPHI, not just the provider who rendered the reproductive healthcare.

(45 CFR 164.502)

- *If you are covered by HIPAA and have RPHI, you need to comply with the rule unless the rule is modified or a court blocks its enforcement.*

Legality of Reproductive Health Care

Prohibition on use or disclosure of RPHI only applies if:

- Activity is in connection with a person seeking, obtaining, providing or facilitating reproductive healthcare (i.e., “expressing interest in, using, performing, furnishing, paying for, disseminating info about, arranging, insuring, administering, authorizing, providing coverage for or otherwise taking action to engage in reproductive health care.”), and
- Covered entity or business associate determines one of following exist:
 - The reproductive care is lawful under the state law and circumstances when rendered; or
 - The reproductive care is protected, required or authorized by federal law.
 - Care provided by another is presumed lawful unless the covered entity or business associate:
 - Has actual knowledge that the care was not lawful; or
 - Factual info provided by person requesting use or disclosure of reproductive PHI demonstrates a substantial factual basis that the care was not lawful.

(45 CFR 164.502(a)(5))

✓ *Rule does not protect illegal activity.*

Purpose for Disclosure of RPHI

- Covered entity and business associate may not use or disclose PHI to:
 - Conduct a criminal, civil or administrative investigation into any person for the mere act of seeking, obtaining, providing or facilitating reproductive healthcare;
 - Impose criminal, civil or administrative liability on any person for the mere act of seeking, obtaining, providing or facilitating reproductive healthcare; or
 - Identify any person for foregoing purposes.
- Covered entity and business associate may use or disclose RPHI for other purposes, e.g.,
 - Treatment, payment or healthcare operations.
 - Investigations or prosecutions that are not for purposes of imposing liability for seeking or obtaining reproductive care.
 - Other permitted purposes.

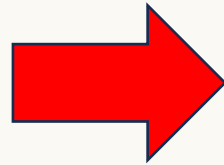
(45 CFR 164.502(a)(5)(iii))

✓ *But only if reproductive healthcare was legal.*

Reproductive Health Rule: Required Attestation

- Covered entity or business associate may not use or disclose reproductive care PHI for **these purposes** without first obtaining a required attestation from the person seeking the PHI.

(45 CFR 164.509)



- Uses or disclosures for health oversight activities. (164.512(d))
 - e.g., govt agencies, licensing, audits, etc.
- Disclosures for judicial and administrative proceedings. (164.512(e))
 - e.g., court orders, subpoenas, warrants, etc.
- Disclosures for law enforcement purposes. (164.512(f))
 - e.g., warrant, police request to locate victim or suspect, report crime on premises, report victim of crime, etc.
- Disclosures to coroners and medical examiners. (164.512(g)(1))

Reproductive Health Rule: Required Attestation

Valid attestation =

- Description of info requested, including name of patient whose info was sought or description of class of such persons.
- Name or description of class of persons requested to make the disclosure.
- Statement that the use or disclosure is not for purpose prohibited by the rule, i.e., criminal, civil or administrative liability.
- Statement that person may be criminally liable under 42 USC 1320d-6 for improperly obtaining or disclosing info in violation of HIPAA.
- Signature of person requesting disclosure.
- Does not contain additional elements.
- Generally, cannot be combined with other documents.

(45 CFR 164.509(b)-(c)).

Reproductive Health Rule: OCR Model Attestation



Model Attestation for a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

When a HIPAA covered entity¹ or business associate² receives a request for protected health information (PHI)³ potentially related to reproductive health care,⁴ it must obtain a signed attestation that clearly states the requested use or disclosure is not for the prohibited purposes described below, where the request is for PHI for any of the following purposes:

- Health oversight activities⁵
- Judicial or administrative⁶ proceedings
- Law enforcement⁷
- Regarding decedents, disclosures to coroners and medical examiners⁸

Prohibited Purposes. Covered entities and their business associates may not use or disclose PHI for 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 lawful reproductive health care.
- (2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- (3) To identify any person for any purpose described in (1) or (2).⁹

The prohibition applies when the reproductive health care at issue (1) is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided, (2) 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, or (3) is provided by another person and presumed lawful.¹⁰

Model Instructions

Information for the Person Requesting the PHI

- By signing this attestation, you are verifying that you are not requesting PHI for a prohibited purpose and acknowledging that criminal penalties may apply if untrue.¹¹
- You may not add content that is not required or combine this form with another document except where another document is needed to support your statement that the requested disclosure is not for a prohibited purpose.¹² For example, if the requested PHI is potentially related to reproductive health care that was provided by someone other than the covered entity or business associate from whom you are requesting the PHI, you may submit a document that supplies information that demonstrates a

- Available at <https://www.hhs.gov/sites/default/files/model-attestation.pdf>.

Problems with the Rule



- Forces provider or business associate to make determinations about legality of care that was rendered.
- Forces provider to fight subpoenas, warrants, court orders, etc., seeking RPHI about care that provider or business associate believes was legal.
 - “[T]he prohibition [on the Rule] would preempt state or other laws requiring a regulated entity to use or disclose PHI in response to a court order or other type of legal process for a purpose prohibited under the proposed rule.” (89 FR 33010).
 - “A regulated entity ... would not be prohibited from disclosing an individual’s PHI when subpoenaed by law enforcement for the purpose of investigating such allegations, assuming that law enforcement provided a valid attestation and met the other conditions of the applicable permission.” (89 FR 32995)

Problems with the Rule



“For example, a regulated entity receives an attestation from a Federal law enforcement official, along with a court ordered warrant demanding PHI potentially related to reproductive health care. The law enforcement official represents that the request is about reproductive health care that was not lawful under the circumstances in which such health care was provided, but the official will not divulge more information because they allege that doing so would jeopardize an ongoing criminal investigation. In this example, if the regulated entity itself provided the reproductive health care and, based on the information in its possession, reasonably determines that such health care was lawful under the circumstances in which it was provided, the regulated entity may not disclose the requested PHI.” (89 FR 33032; *see also id.* at 33015)

Problems with the Rule



The new rule “potentially put[s] [providers and business associates] in situations where they need to choose between complying with a court order and impermissibly disclosing PHI....”

“*Response:* ...[A]ny burden the attestation may impose on persons requesting PHI is outweighed by the privacy interests that this final rule is designed to protect.” (89 FR 33033)

Reproductive Health Rule: Additional 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.
 - Fetuses are not protected by HIPAA.
 - Mothers are.
- *Public health* defined to exclude activities to investigate or impose criminal, civil or administrative liability for the mere act of seeking, obtaining, providing or facilitating reproductive care.
 - Exception that would allow disclosures for public health activities does not apply to the extent the activity is intended to investigate or assert claims based on obtaining reproductive health care.

(45 CFR 160.103)

Reproductive Health Rule: Personal Representatives

- Personal representative may generally access patient's PHI.

(45 CFR 164.504(g)(1))

- Notwithstanding any state law to the contrary, a covered entity may elect not to treat person as the personal representative if both the following apply:
 - Covered entity has reasonable belief that:
 - Patient has been or may be subjected to domestic violence, abuse or neglect by such person, or
 - Treating person as the personal rep could endanger the individual; and
 - Covered entity decides that it is not in the best interest of the patient to treat the person as the patient's personal representative.
- Not a “reasonable belief” if the basis for belief is that the person is seeking reproductive care for the patient at the patient's request.

(45 CFR 164.504(g)(5))

Civil Penalties (if regulated by HIPAA)

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"> • \$141* to \$71,162* per violation • Up to \$2,067,813* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	<ul style="list-style-type: none"> • \$1,379* to \$71,162* per violation • Up to \$2,067,813* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none"> • \$14,232* to \$71,162* per violation • Up to \$2,067,813* per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none"> • \$71,162 to \$2,134,831* per violation • Up to \$2,134,831* per type per year • Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

Criminal Penalties (even if not regulated by HIPAA)

Applies if individuals obtain or disclose PHI from covered entity without authorization, e.g., submit false attestation.

Conduct	Penalty
Knowingly obtain info in violation of the law	\$50,000 fine 1 year in prison
Committed under false pretenses	100,000 fine 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	\$250,000 fine 10 years in prison

(42 USC 1320d-6(a))

On the other hand...

- If refuse to produce info in response to subpoena, warrant, court order:
 - Potential civil, criminal, or administrative penalties, e.g.,
 - Contempt
 - Obstruction of justice
 - Failure to respond to process
 - Cost of defending against charges or disclosure.
 - No insurance coverage?



OCR Resources

<https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/index.html>

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics —

HIPAA and Part 2

Change Healthcare Cybersecurity
Incident FAQs

HIPAA and COVID-19

**HIPAA and Reproductive
Health** —

HIPAA and Final Rule Notice

HIPAA and Telehealth

HIPAA and FERPA

Research

HIPAA and Reproductive Health

Final Rule HIPAA Privacy Rule to Support Reproductive Health Care Privacy

On April 22, 2024, OCR issued a Final Rule, entitled *HIPAA Privacy Rule to Support Reproductive Health Care Privacy*. The Final Rule strengthens the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by prohibiting the disclosure of protected health information related to lawful reproductive health care in certain circumstances. HHS issued this Final Rule after hearing from communities that changes were needed to better protect patient confidentiality and prevent medical records from being used against people for providing or obtaining lawful reproductive health care. This Final Rule bolsters patient-provider confidentiality and helps promote trust and open communication between individuals and their health care providers or health plans, which is essential for high-quality health care.

[Press Release](#)

[To read the Fact Sheet](#) ([en español](#))

HIPAA Disclosures per Administrative Request



HIPAA

Disclosures per Administrative Requests

- HIPAA allows disclosures for certain law enforcement requests, including but not limited to:
 - “(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.”

(45 CFR 164.512(f)(1)(C))

- ✓ *Clarifies that “administrative request” exception only applies if the response is required by law, not just because the agent requests the info.*

HIPAA Changes



HIPAA

Proposed Privacy Rule Changes

Proposed rule published 1/21/21; still waiting...

- Strengthens individual's right of access.
 - Individuals may take notes or use other personal devices to view and capture images of PHI.
 - Must respond to requests to access within 15 days instead of 30 days.
 - Must share info when directed by patient.
 - Additional limits to charges for producing PHI.
- Facilitates individualized care coordination.
- Clarifies the ability to disclose to avert threat of harm.
- Not required to obtain acknowledgment of Notice of Privacy Practices.
- Modifies content of Notice of Privacy Practices.

(86 FR 6446 (1/21/21))

HIPAA

Proposed Security Rule Changes

- Proposed rule published 1/6/25
- Strengthens security standards
 - Remove “addressable” standards; all standards are required.
 - Written documentation of all security rule policies, procedures, plans and analyses.
 - At least every 12 months must:
 - Inventory tech assets and develop/update network map.
 - Risk analysis with updated requirements.
 - Review and update risk management plan.
 - Review and test policies, plans and processes.
 - Security training.
 - Compliance audit.
 - Obtain verification of business associate compliance.
 - New technical requirements, e.g., patches, upgrades, policies, access, incident response, contingency plans, penetration testing, encryption, anti-malware protection, multi-factor authentication, etc.
 - Written policies for sanctioning employees.

(90 FR 898)

HIPAA Proposed Security Rule Changes

<https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>

Health Information Privacy

[HIPAA for Individuals](#)[Filing a Complaint](#)[HIPAA for Professionals](#)[Newsroom](#)

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [The Security Rule](#) > [HIPAA Security Rule NPRM](#) > HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cyber...

[HIPAA for Professionals](#)[Regulatory Initiatives](#)[Privacy](#) +[Security](#) +[Breach Notification](#) +[Compliance & Enforcement](#) +[Special Topics](#) +[Patient Safety](#)[Covered Entities & Business Associates](#) +[Training & Resources](#)[FAQs for Professionals](#)

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

Fact Sheet

On December 27, 2024, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA and Online Tracking Technologies



HIPAA and Online Tracking

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>



About HHS Programs & Services Grants & Contracts Laws & Regulation

Health Information Privacy

HIPAA for Individuals

Filing a Complaint

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance Materials](#) > U

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics +

Patient Safety +

Use of tracking technologies on websites and mobile apps may violate HIPAA, e.g.,

- Cookies
- Web beacons
- Tracking pixels
- Session replay scripts
- Fingerprint scripts
- IP addresses
- Geolocations

1. Does the data contain individually identifiable info that relates to past, present, or future health, healthcare or payment?
2. If so, does HIPAA permit the use or disclosure without patient authorization?

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

On March 18, 2024, OCR updated this guidance to increase clarity for regulated entities and the public.

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to

HIPAA and Online Tracking

“On June 20, 2024, [a district court] issued an order declaring unlawful and vacating ... the guidance to the extent it provides that HIPAA obligations are triggered in ‘circumstances where an online technology connects (1) an individual’s IP address with (2) a visit to a[n] [unauthenticated public webpage] addressing specific health conditions or healthcare providers.’”
See Am. Hosp. Ass’n v. Becerra, 2024 WL 3075865 (N.D. Tex. June 20, 2024).



[About HHS](#) [Programs & Services](#) [Grants & Contracts](#) [Laws & Regulation](#)

Health Information Privacy

[HIPAA for Individuals](#)

[Filing a Complaint](#)

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance Materials](#) > U

[HIPAA for Professionals](#)

[Regulatory Initiatives](#)

[Privacy](#) +

[Security](#) +

[Breach Notification](#) +

[Compliance & Enforcement](#) +

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

Online Tracking Lawsuits

NC Health System Agrees to Pay \$6.6M in Web Tracking Case

Novant Health Is Among Latest Organizations Opting to Settle Patient Privacy Claims

Marianne Kolbasuk McGee (HealthInfoSec) • January 16, 2024

Share Tweet Share Credit Eligible

Get Permission

npr Illinois 91.9 UIS The Capital's Community & News Service

NPR Illinois
Fresh Air

Small western Illinois hospitals face federal lawsuits over online tracking

Tri States Public Radio | By Jane Carlson
Published September 19, 2024 at 1:13 PM CDT

Share

Possible Theories

- Negligence per se based on violation of statute
- Unfair or deceptive trade practices acts
- Federal and state wire-tapping laws
- Negligent misrepresentation
- Invasion of privacy
- Breach of contract
- Others?

42 CFR Part 2 Rules

**SUBSTANCE USE
DISORDER
RECORDS**



Substance Use Disorder Records

New rule:

- Issued 2/8/24.
- Effective 4/16/24.
- **Enforced 2/16/26.**

(89 FR 12472)

Applies to:

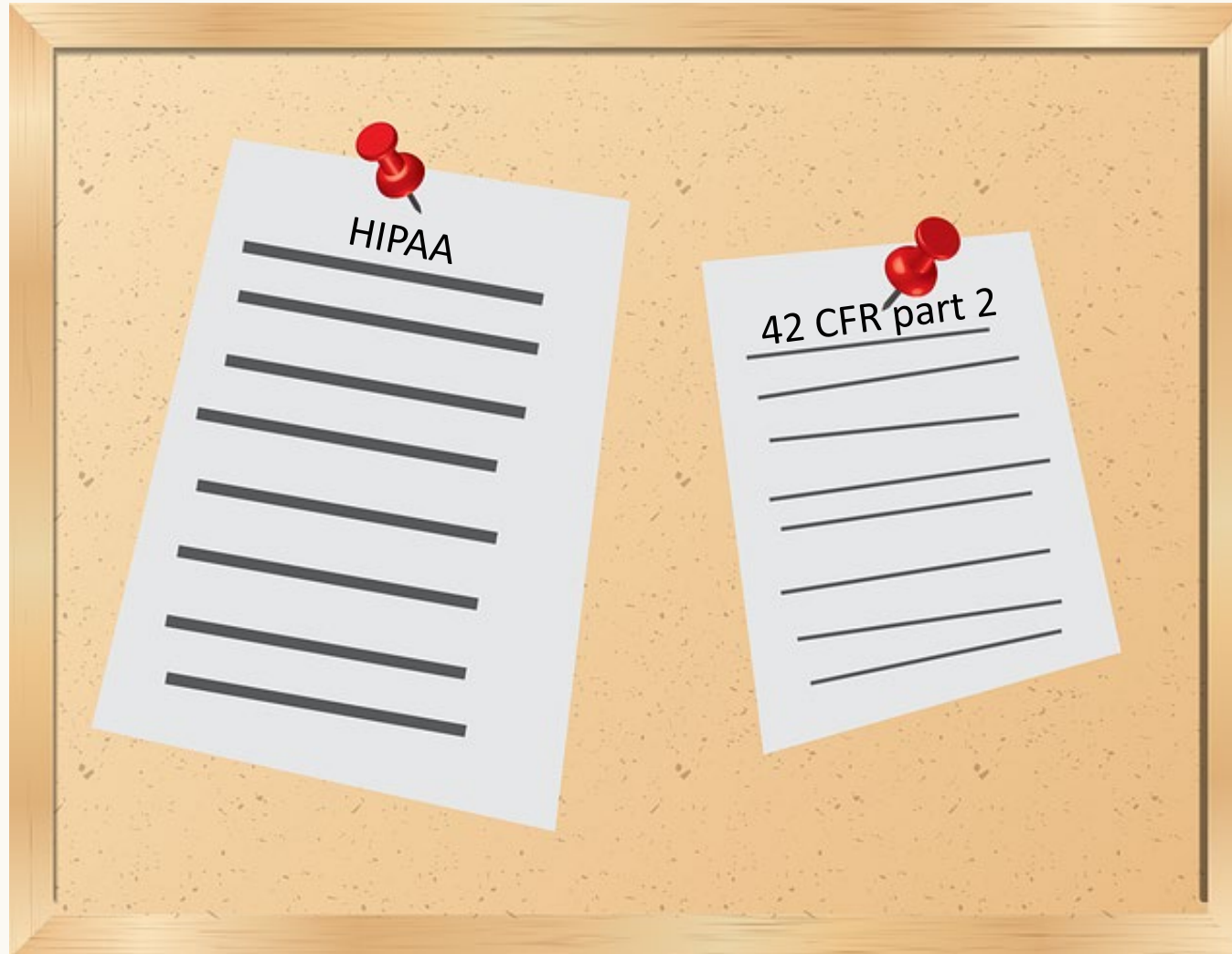
- Federally assisted SUD programs.
- Recipients of SUD records from such a program.

Aligns 42 CFR part 2 with HIPAA.

- HIPAA enforcement applies to Part 2 violations.
- Allows single consent for uses or disclosures for treatment, payment or healthcare operations.
- HIPAA-covered entities and business associates receiving SUD info under consent may use or disclose consistent with HIPAA.
- Must provide HIPAA-like notice of privacy practices (NPP) and update HIPAA NPP.

(42 CFR part 2)

HIPAA and SUD Rules: Notice of Privacy Practices



HIPAA and 42 CFR part 2 Notice of Privacy Practices

- By **2/16/26**, must update Notice of Privacy Practices (“NPP”) to address:
 - Changes to substance use disorder records required by 42 CFR part 2.
 - Changes caused by Reproductive Health Rule.

(45 CFR 164.520(a)(2))

- ✓ *Check applicable regulations when drafting updated NPP.*
- ✓ *Watch for new NPP requirements when final HIPAA revisions are published.*
- ✓ *OCR plans to publish model NPP.*

FTC and Data Security





[Home](#) » [News & Events](#) » [Media Resources](#) » [Protecting Consumer Privacy and Security](#) » [Privacy and Security Enforcement](#)

Protecting Consumer Privacy and Security

FTC POLICY WORK

PRIVACY AND SECURITY ENFORCEMENT

FINANCIAL PROTECTION

KIDS' PRIVACY

Privacy and Security Enforcement

PRIVACY AND SECURITY ENFORCEMENT

When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up to these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information...

“When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up to these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information...”

► [BLOG POSTS](#)

► [PUBLIC EVENTS](#)

FTC Enforcement of Privacy and Security

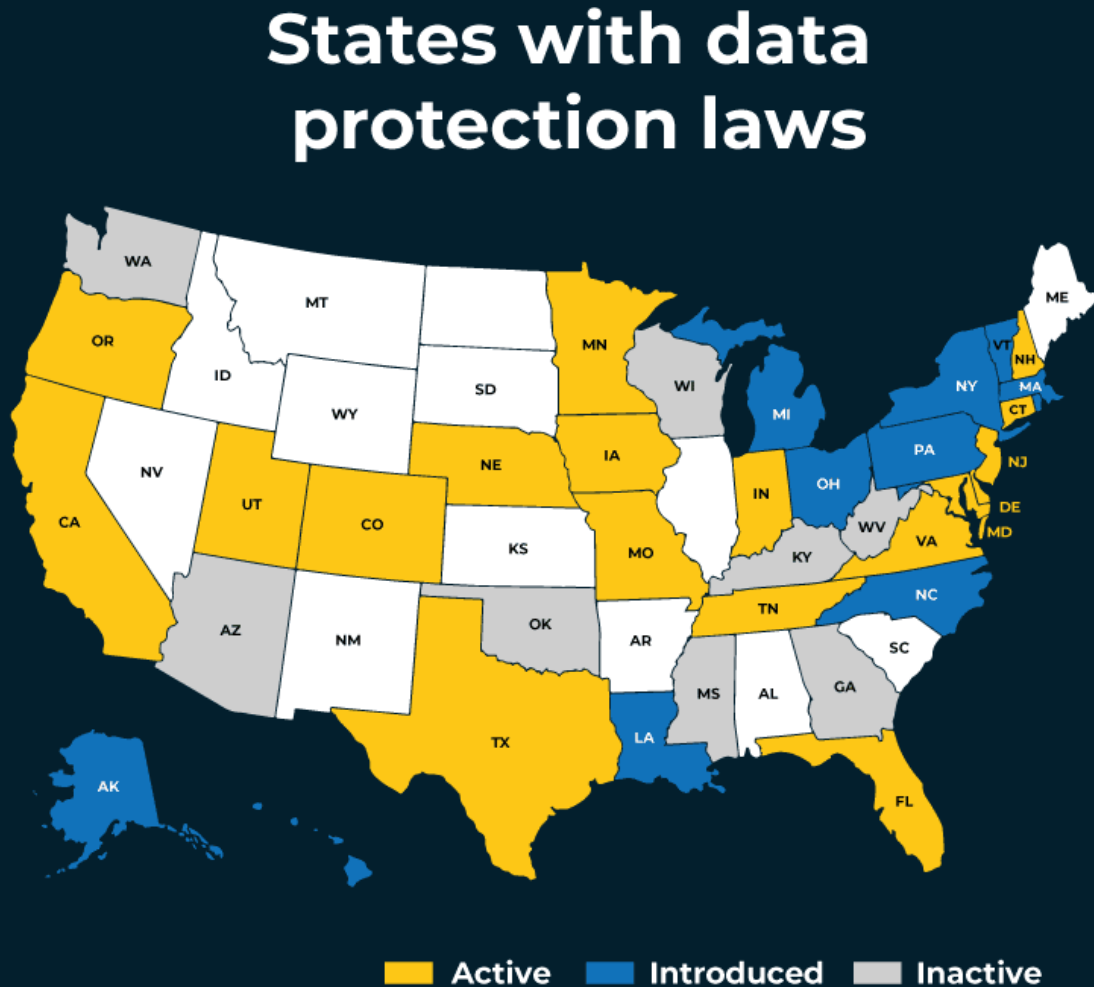
FTC is using FTCA § 5 to go after entities for data security breaches.

- Bars unfair and deceptive trade practices, e.g.,
 - Mislead consumers re security practices.
 - Misusing info or causing harm to consumers.

(<https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement>)

- [Facebook, Inc., In the Matter of](#) (November 7, 2024)
- [Marriott International, Inc. and Starwood Hotels & Resorts Worldwide, LLC, In the Matter of](#) (October 9, 2024)
- [Verkada Inc., U.S. v.](#) (August 30, 2024)
- [FTC v Kochava, Inc.](#) (July 15, 2024)
- [NGL](#) (July 9, 2024)
- [Avast](#) (June 26, 2024)
- [Monument, Inc., U.S. v.](#) (June 7, 2024)
- [Cerebral, Inc. and Kyle Robertson, U.S. v.](#) (May 31, 2024)
- [Blackbaud, Inc.](#) (May 20, 2024)
- [BetterHelp, Inc., In the Matter of](#) (May 6, 2024)
- [Aqua Finance](#) (May 1, 2024)
- [InMarket Media, LLC](#) (May 1, 2024)
- [Ring, LLC](#) (April 23, 2024)
- [X-Mode Social, Inc.](#) (April 11, 2024)
- [Rite Aid Corporation, FTC v.](#) (March 8, 2024)
- [Global Tel Link Corporation](#) (February 23, 2024)
- [Epic Games, In the Matter of](#) (January 10, 2024)
- [CafePress, In the Matter of](#) (January 10, 2024)
- [TransUnion Rental Screening Solutions, Inc. and Trans Union, LLC., FTC and CFPB v.](#) (October 20, 2023)
- [TruthFinder, LLC, FTC v.](#) (October 11, 2023)

State Data Privacy Laws



- *Beware telehealth and other situations in which you may be subject to laws in other states.*
- *Remember HIPAA requires that you comply with the most restrict laws.*

Source: <https://www.securescan.com/articles/records-management/data-privacy-laws-and-compliance/>

Info Blocking Rule

- Applies to “actors”
 - Healthcare providers.
 - Developers or offerors of certified health IT.
 - Not providers who develop their own IT.
 - Health info network/exchange.

(45 CFR 171.101)

- Prohibits info blocking, i.e., practice that is likely to interfere with access, exchange, or use of electronic health info, and
- Provider: knows practice is unreasonable and likely to interfere.
- Developer/HIN/HIE: knows or should know practice is likely to interfere.

(45 CFR 171.103)

Info Blocking Rule Penalties

DEVELOPERS, HIN, HIE

- Complaints to OIG
 - <https://inquiry.healthit.gov/support/plugins/servlet/desk/portal/6>
 - OIG Hotline
- Civil monetary penalties of up to \$1,000,000 per violation

(42 CFR 1003.1420)

HEALTHCARE PROVIDERS

- Final rule issued 6/24/24:
 - Hospitals: loss of status as meaningful user of EHR
 - Providers: loss of status as meaningful user under MIPS
 - ACOs: ineligible to participate.
 - Loss of federal payments.

Info Blocking Rule Guidance

<https://www.healthit.gov/topic/information-blocking>



TOPICS ▾

BLOG

NEWS ▾

DATA

ABOUT ONC ▾



HealthIT.gov > Topics > **Information Blocking**

Information Blocking

Most clinical information is digitized, accessible, and shareable thanks to several technology and policy advances making interoperable, electronic health record systems widely available. In 2016, the 21st Century Cures Act (Cures Act) made sharing electronic health information the expected norm in health care by authorizing the Secretary of Health and Human Services (HHS) to identify "reasonable and necessary activities that do not constitute information blocking." ONC's 2020 Cures Act Final Rule established information blocking exceptions to implement the law.



What Is Information Blocking and to

Artificial Intelligence (AI)



AI in Healthcare

Rapidly developing area of the law; watch for federal and state regulation.

Common uses in healthcare

- Imaging
- Clinical decision support tools
- Research
- Virtual assistant for transcription, administration, or practice management
- Others?

Concerns

- Bias or discrimination
- “Garbage in, garbage out” → incorrect results
- Lack of transparency in algorithms, i.e., “black box” results
- Data privacy
- Others?

AI in Healthcare



Watch for
developments

FEDERAL INITIATIVES

- 2022: Whitehouse Blueprint for AI Bill of Rights
- 2023: Executive Order requiring federal agencies to develop guidelines
- 2023: NIST AI Risk Management Framework
- 2024: Federal actions
 - Bipartisan AI Working Groups and AI Policy Roadmaps
 - Proposed legislation
 - Agency guidance
 - Others

STATE INITIATIVES

- Proposed legislation, e.g.,
 - Disclosure and consent of use in patient encounters
 - Limits on use in utilization review and coverage determinations
 - Others?
- Other considerations
 - Standard of care
 - Informed consent
 - Discrimination

Additional Resources



OCR HIPAA Website

<https://www.hhs.gov/hipaa/for-professionals/index.html>

[HHS](#) > [HIPAA Home](#) > HIPAA for Professionals

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics +

Patient Safety

Covered Entities & Business Associates +

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules



HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

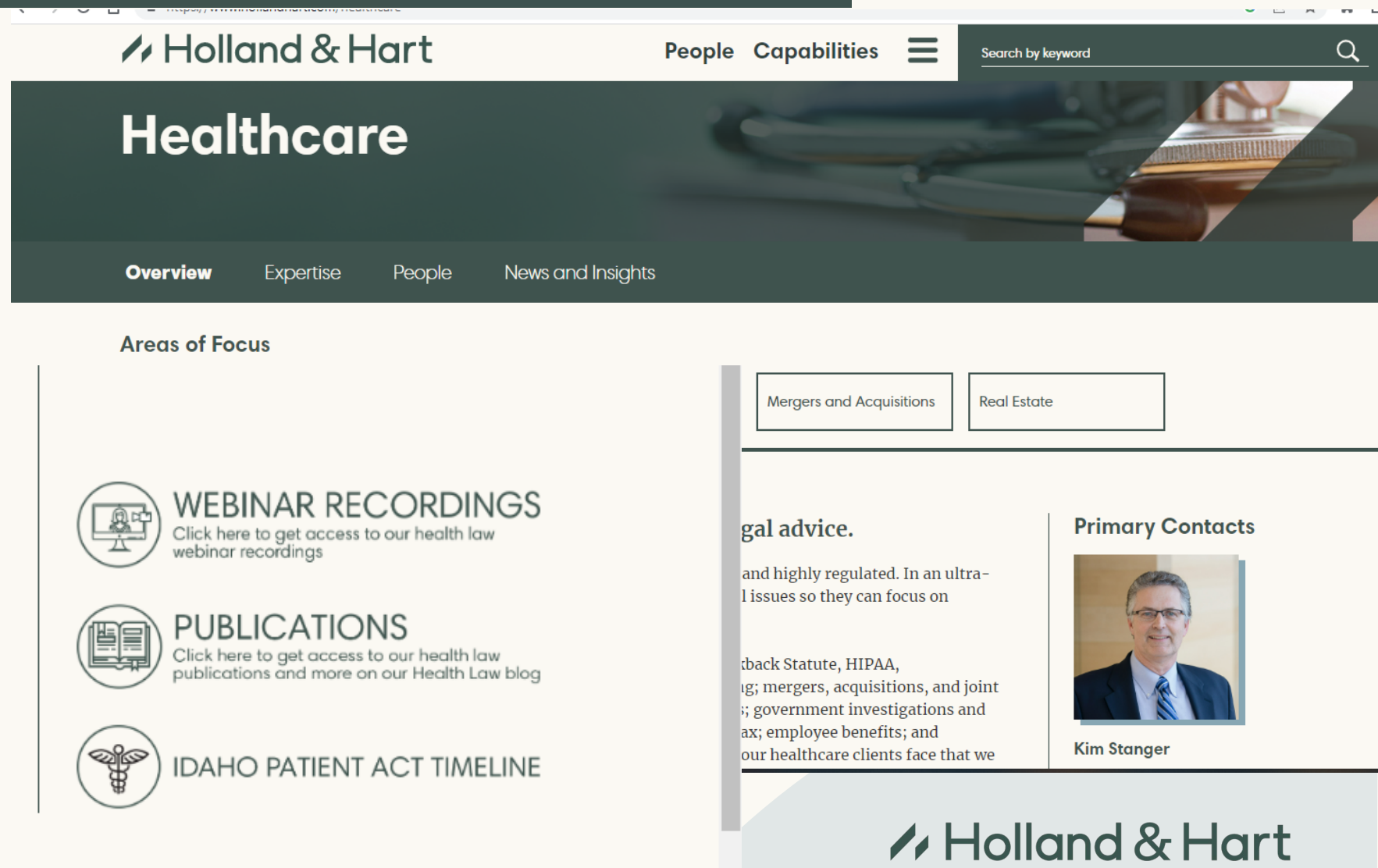
- HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).

[↑ Back to top](#)

HTTPS://WWW.HOLLANDHART.COM/ HEALTHCARE

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other



The screenshot displays the Holland & Hart website's Healthcare section. The header includes the firm's logo, navigation links for 'People' and 'Capabilities', and a search bar. The main banner features the word 'Healthcare' in large white text over a background image of a stethoscope. Below the banner is a navigation bar with links for 'Overview', 'Expertise', 'People', and 'News and Insights'. The 'Areas of Focus' section contains three items: 'WEBINAR RECORDINGS' with a monitor icon, 'PUBLICATIONS' with a book icon, and 'IDAHO PATIENT ACT TIMELINE' with a caduceus icon. To the right, there are buttons for 'Mergers and Acquisitions' and 'Real Estate'. Further down, a 'Primary Contacts' section features a photo of Kim Stanger, a man in a suit and glasses, with his name listed below. The footer of the page shows the Holland & Hart logo.

Holland & Hart

People Capabilities

Search by keyword

Healthcare

Overview Expertise People News and Insights

Areas of Focus

Mergers and Acquisitions Real Estate

WEBINAR RECORDINGS
Click here to get access to our health law webinar recordings


PUBLICATIONS
Click here to get access to our health law publications and more on our Health Law blog

IDAHO PATIENT ACT TIMELINE

gal advice.
and highly regulated. In an ultra-
l issues so they can focus on

back Statute, HIPAA,
g; mergers, acquisitions, and joint
; government investigations and
ax; employee benefits; and
our healthcare clients face that we

Primary Contacts


Kim Stanger

Holland & Hart

Questions?



Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com