



# HIPAA AND DATA PRIVACY UPDATE

Kim Stanger

(6-24)

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

- New HIPAA Rules and Guidance
  - Data Tracking Technologies
  - Reproductive Rights
  - Additional Tweaks
  - Proposed Rules
- Substance Use Disorder Rules
- Notice of Privacy Practices Changes
- FTC, SEC and State Data Privacy Laws and Actions
- Cybersecurity Resources
- Information Blocking Rule Penalties
- Data Privacy Concerns in AI



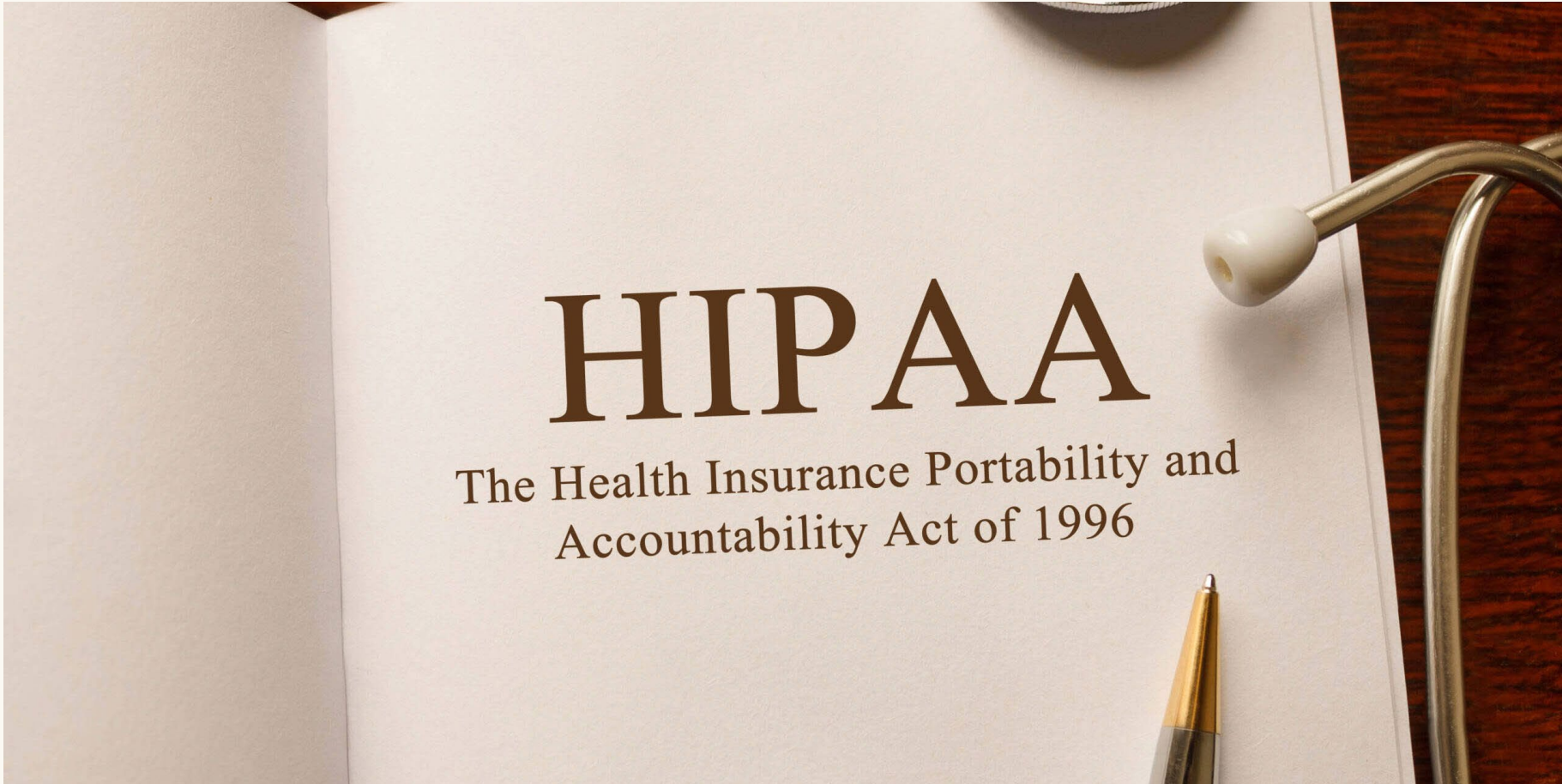
# Resources

- .ppt slides
- Stanger, *Avoiding HIPAA Penalties: A Checklist for Covered Entities*, <https://www.hollandhart.com/hipaa-checklist-covered-entities>
- OCR, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>
- OCR, *HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy: Fact Sheet*, <https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html>
- Cybersecurity resources identified in slides.

# Preliminaries

- Presentation will be recorded and available on our website, <https://www.hhhealthlawblog.com/webinar-recordings-and-presentations/>
- If you have questions,
  - Submit with chat feature, or
  - E-mail me at [kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com)

# HIPAA



# HIPAA Criminal Penalties

Applies if individuals obtain or disclose PHI from covered entity without authorization.

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))

# HIPAA Civil Penalties

Watch for new rule that will give individuals a portion of settlements or penalties. (87 FR 19833 (4/6/22))

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"><li>• \$127* to \$63,973* per violation</li><li>• Up to \$1,919,173* per type per year</li><li>• <b>No penalty if correct w/in 30 days</b></li><li>• OCR may waive or reduce penalty</li></ul>
Violation due to reasonable cause	<ul style="list-style-type: none"><li>• \$1,280* to \$63,973* per violation</li><li>• Up to \$1,919,173* per type per year</li><li>• <b>No penalty if correct w/in 30 days</b></li><li>• OCR may waive or reduce penalty</li></ul>
<b>Willful neglect,</b> but correct w/in 30 days	<ul style="list-style-type: none"><li>• \$12,794* to \$63,973* per violation</li><li>• Up to \$1,919,173* per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>
<b>Willful neglect,</b> but do not correct w/in 30 days	<ul style="list-style-type: none"><li>• \$63,973 to \$1,919,173* per violation</li><li>• Up to \$1,919,173* per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>

(45 CFR 102.3, 160.404; 85 FR 2879)



# Recent HIPAA Resolutions

<https://www.hhs.gov/hipaa/newsroom/index.html>

Date	Conduct	Resolution
4/1/24	Essex Residential Care failed to give personal representative timely access to records.	\$100,000
3/29/24	Phoenix Healthcare failed to provide personal representatives timely access to records.	\$35,000
2/6/24	Montefiore Medical Center failed to protect against malicious insider selling info.	\$4,750,000
11/20/23	St. Joseph's Medical Center disclosed PHI to news reporter.	\$80,000
10/31/23	Doctor's Management Services hit by ransomware affecting 206,695 persons.	\$100,000
9/11/23	L.A. Care Plan failed to secure patient portal, perform risk analysis, and mailed ID cards to wrong patients. Affected 2500+ persons.	\$1,300,000
8/24/23	UnitedHealthcare failed to timely provide copy of records.	\$80,000
6/28/23	iHealth Solutions' PHI of 267 persons was exfiltrated by unauthorized persons.	\$75,000
6/15/23	Yakima Valley Hospital security guards snooping through records of 419 persons.	\$240,000
6/4/23	Manesa Health Center disclosed PHI in response to negative online reviews.	\$30,000
5/16/23	MedEvolve (business associate) left server unsecured exposing PHI of 230,572 persons.	\$350,000
5/8/23	David Mente, LPC, failed to provide father with records of three minor children.	\$15,000
2/2/23	Banner Health hacked, exposing PHI of 2,810,000 persons; failure to implement security rule.	\$1,250,000
1/22/23	Life Hope Labs failed to provide personal rep with records of deceased patient	\$16,500

# Recent HIPAA Resolutions

<https://www.hhs.gov/hipaa/newsroom/index.html>

Date	Conduct	Resolution
4/1/24	Essex Residential Care failed to provide personal representative timely access to records.	\$100,000
3/29/24	Phoenix Healthcare failed to provide personal representatives timely access to records.	\$35,000
2/6/24	Montefiore Medical Center failed to protect PHI by selling info.	\$4,750,000
11/20/23	St. Joseph's Medical Center failed to protect PHI by selling info.	\$80,000
10/31/23	Doctor's Management Services failed to protect PHI by selling info to 5 persons.	\$100,000
9/11/23	L.A. Care Plan failed to protect PHI by sending and mailed ID cards to wrong patients.	\$1,300,000
8/24/23	UnitedHealthcare failed to protect PHI by selling info to 5 persons.	\$80,000
6/28/23	iHealth Solutions' failed to protect PHI by selling info to 5 persons.	\$75,000
6/15/23	Yakima Valley Hospital failed to protect PHI by selling info to 419 persons.	\$240,000
6/4/23	Manesa Health Center failed to protect PHI by selling info to 5 persons.	\$30,000
5/16/23	MedEvolve (business) failed to protect PHI by selling info to a group of 230,572 persons.	\$350,000
5/8/23	David Mente, LPC, failed to provide father with records of three minor children.	\$15,000
2/2/23	Banner Health hacked, exposing PHI of 2,810,000 persons; failure to implement security rule.	\$1,250,000

## Top HIPAA Risks



1. Cyberattacks
2. Security rule violations
3. Right of access violations

# HIPAA

## Avoiding Civil Penalties

- ✓ Appoint qualified privacy/security officers
- ✓ Have required policies and safeguards in place.
  - Privacy Rule
    - Use and disclosure rules
    - Individual rights
  - Security Rule
  - Breach Notification Rule
- ✓ Have compliant forms (e.g., authorization, Notice of Privacy Practices, etc.)
- ✓ Perform and document periodic security risk assessment.
- ✓ Execute business associate agreements.
- ✓ Train members of your workforce and document training.
- ✓ Respond immediately to mitigate and correct any violation.
- ✓ Timely report breaches if required.

(45 CFR part 164; <https://www.hollandhart.com/hipaa-checklist-covered-entities>)

*No “willful neglect” = No penalties if correct violation within 30 days.*

# HIPAA Enforcement

- Must self-report breaches of unsecured protected health info
  - To affected individuals.
  - To HHS.
  - To media if breach involves > 500 persons.
- In future, individuals may recover portion of penalties or settlement.
  - On 4/6/22, HHS issued notice soliciting input. (87 FR 19833)
- State attorney general can bring lawsuit.
  - \$25,000 fine per violation + fees and costs
- Must sanction employees who violate HIPAA.
  - In 10/23, HHS issued bulletin re sanctioning workforce members.
- Possible lawsuits by affected individuals or others.
  - See, e.g., recent class action lawsuits over privacy violations.



Now applies to violations of SUD info

# HIPAA Privacy Rule Right of Access



Search

About HHS Programs & Services Grants & Contracts Laws & Regulations

Home > About > News > HHS Office for Civil Rights Imposes a Civil Monetary Penalty on New Jersey Nursing Facility for Failing to Provide Timely Access to P...



FOR IMMEDIATE RELEASE  
April 1, 2024

Contact: HHS Press Office  
202-690-6343  
[media@hhs.gov](mailto:media@hhs.gov)

## HHS Office for Civil Rights Imposes a Civil Monetary Penalty on New Jersey Nursing Facility for Failing to Provide Timely Access to Patient Records

*Essex Residential Care, LLC, to pay \$100,000 after failing to comply with HIPAA Right of Access*

48<sup>th</sup> case  
under OCR's  
Right of  
Access  
Initiative

**\$100,000 Civil Monetary Penalty**

- Ensure you timely respond to patient's or personal rep's request to access records.
  - Applies to designated record set.
    - Limited exceptions.
    - Includes records from other providers.
  - 30-day / 60-day time limit.\*
    - Proposed Rule would shorten.
    - Beware Info Blocking Rule
- Must send e-PHI to third party identified by patient.
- May charge reasonable cost-based fee.  
(45 CFR 164.524)

# HIPAA Privacy Rule Right of Access

- Review OCR Guidance at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>.
  - General right of access
  - “Designated record set”
  - Exceptions
  - Form and format for access
  - Timelines
  - Fees
  - Denial of access
  - Patient’s right to direct ePHI to another person
  - FAQs

## Individuals’ Right under HIPAA to Access their Health Information 45 CFR § 164.524

This guidance remains in effect only to the extent that it is consistent with the court's order in *Ciox Health, LLC v. Azar*, No. 18-cv-0040 (D.D.C. January 23, 2020), which may be found at [https://ecf.dcd.uscourts.gov/cgi-bin/show\\_public\\_doc?2018cv0040-51](https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2018cv0040-51). More information about the order is available at <https://www.hhs.gov/hipaa/court-order-right-of-access/index.html>. Any provision within this guidance that has been vacated by the *Ciox Health* decision is rescinded.

[Newly Released FAQs on Access Guidance](#)

[New Clarification – \\$6.50 Flat Rate Option is Not a Cap on Fees for Copies of PHI](#)

### Introduction

Providing individuals with easy access to their health information empowers them to be more in control of decisions regarding their health and well-being. For example, individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. With the increasing use of and continued advances in health information technology, individuals have ever expanding and innovative opportunities to access their health information electronically, more quickly and easily, in real time.

# HIPAA and Online Tracking Technologies



# Online Tracking Concerns

The Markup  
(6/16/22)



The HIPAA Journal is tl  
and indep

[Become HIPAA Compliant »](#) [HIPAA News »](#) [HIPAA Compliance Checklist](#) [Latest HIPAA Updates »](#) [HIPAA Training »](#) [About Us »](#)

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

Posted By Steve Alder on Jan 20, 2022

An \$18.4 million settlement has been approved that resolves a class action lawsuit against Mass General Brigham over the use of cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.

The defendants in the case operate informational websites that provide information about the healthcare services they provide and the programs they operate. Those websites can be accessed by the general public and do not require visitors to register or create accounts.

The lawsuit was filed against Partners Healthcare System, now Mass General Brigham, by two plaintiffs – John Doe and Jane Doe – who alleged the websites contained third party analytics tools, cookies, and pixels that caused their web browsers to divulge information about their use of the Internet, and that the information was transferred and sold to third parties without their consent.

Pixel Hunt

## Facebook Is Receiving Sensitive Medical Information from Hospital Websites

Anson Chan

Experts say some hospitals' use of an ad tracking tool may violate a federal law protecting health information

By [Todd Feathers](#), [Simon Fondrie-Teitler](#), [Angie Waller](#), and [Surya Mattu](#)

A tracking tool installed on many hospitals' websites has been collecting patients' sensitive health information—including details about their medical conditions, prescriptions, and doctor's appointments—and sending it to Facebook.

See our data here.

GitHub

The Markup tested the websites of [Newsweek's](#) top 100 hospitals in America. On 33 of them we found the tracker, called the Meta Pixel, sending Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. The data is connected to an IP address—an identifier that's like a computer's mailing address and can generally be linked to a specific individual or household—creating an intimate receipt of the appointment request for Facebook.

A Third of Top Hospitals' Websites Sent Patient Data to



# HIPAA and Online Tracking

- 12/1/22: OCR bulletin on *Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*
- 7/20/23: FTC and OCR letter to 130 hospitals warn hospitals and telehealth providers that use of online tracking technologies integrated in websites and mobile apps may violate HIPAA privacy and security rules.
- 11/2/23: AHA, Texas Hosp. Ass'n, and others sued OCR/HHS to bar enforcement of 12/22 guidance.
- 3/18/24: OCR updated guidance re *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*

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

## Health Information Privacy

[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 Ass...](#)

[HIPAA for Professionals](#)

[Regulatory Initiatives](#)

[Privacy](#) +

[Security](#) +

[Breach Notification](#) +

[Compliance & Enforcement](#) +

[Special Topics](#) +

[Patient Safety](#) +



## 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

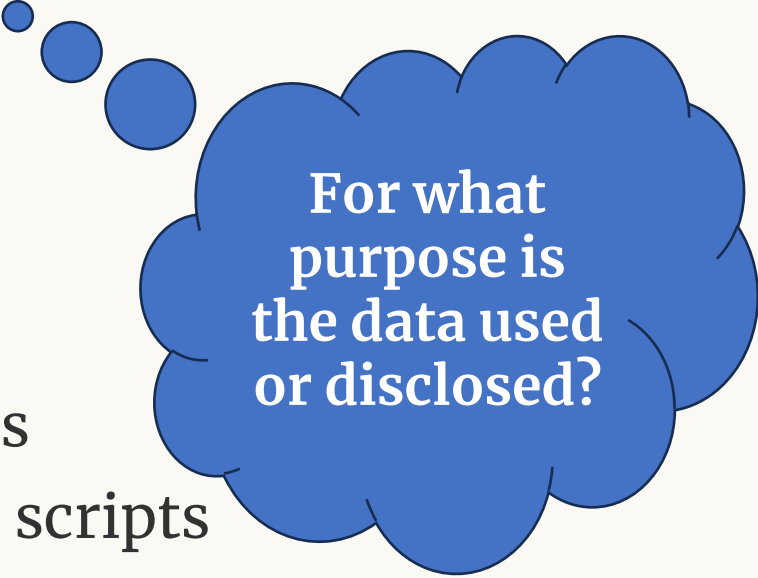
### Applies to all:

- Covered entities with website utilizing tracking technologies
- Business associates of such covered entities, including vendors who assist with websites and tracking technologies

# Online Tracking Technologies

## WEBSITES

- Cookies
- Web beacons
- Tracking pixels
- Session replay scripts
- Fingerprinting scripts
- Others?



For what purpose is the data used or disclosed?

## MOBILE APPS

PHI in app may include:

- Info uploaded to app
- IP address
- Device ID
- Fingerprints
- Network location
- Geolocation
- Advertising ID

# HIPAA and Online Tracking

- “The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI)... **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.”

(OCR Online Tracking Guidance at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>).

# Analysis: HIPAA and Use of Data

- Is it from a covered entity or business associate?
- Is it protected health info (PHI)?
  - Is it individually identifiable?
  - Does it relate to health, healthcare or payment?
- Is the use or disclosure permitted without authorization?
  - By covered entity?
    - e.g., healthcare operations, research, etc.?
  - By business associate or subcontractor?
    - For covered entity for permissible purpose, e.g., healthcare operations, research, etc.?
    - For business associate's own "management and administration" purposes?
    - Permitted by the business associate agreement?
- Is use consistent with, e.g., Notice of Privacy Practices or agreements with the patient?
- Has appropriate authorization been obtained?

## Includes, e.g.:

- Names, addresses, phone numbers
- E-mail and IP addresses
- URLs
- Device identifiers
- Any other unique identifying number, characteristic or code

(45 CFR 164.514(b)(2))

# Covered Entity: Health Care Operations

“[A]ny of the following activities of the covered entity to the extent that the activities are related to covered functions:

- “Conducting quality assessment and improvement activities...; patient safety activities ...; population-based activities ...; case management and care coordination, ... and related functions that do not include treatment;
- “Reviewing the competence or qualifications of health care professionals [and] conducting training programs ...;
- “Conducting or arranging for medical review, legal services, and auditing...;
- “Business planning and development...;
- “Business management and general administrative activities...; [and]
- “Creating de-identified health info or a limited data set...;”

(45 CFR 164.501)

✓ *There are limits to “health care operations.”*

# Covered Entity: Health Care Operations

- “The preamble [to the HIPAA final rule] listed certain activities that would not be considered health care operations because they were sufficiently unrelated to treatment and payment to warrant requiring an individual to authorize such use or disclosure. Those activities included:
    - “marketing of health and non-health items and services;
    - “disclosure of PHI for sale, rent or barter;
    - “use of PHI by a non-health related division of an entity; and
    - “fundraising.”
- (65 FR 82490)
- others?

# Business Associate: Use of PHI

Business associate may use PHI:

- Only as permitted by the BAA, not for other purposes.
- Only to the extent the covered entity could use or disclose the PHI (e.g., for the covered entity's treatment, payment, or healthcare operations), except business associate may use the PHI for following purposes if permitted by BAA:
  - For data aggregation services relating to the healthcare operations of the covered entity; and/or
  - For the proper management and administration of the business associate.
- To deidentify the PHI if permitted by the covered entity.

(45 CFR 164.502(e) and .504(e))

- “[B]usiness associates, with limited exceptions, cannot use PHI for their own purposes...” (<https://www.hhs.gov/hipaa/for-professionals/faq/276/can-business-associates-use-protected-health-information-for-marketing/index.html>)



# Business Associate: Use of PHI

“We agree that PHI should only be used by business associates for the purposes identified in the business associate contract. We address the issue of data mining by requiring that the business associate contract explicitly identify the uses or disclosures that the business associate is permitted to make with the PHI. Aside from disclosures for data aggregation and business associate management, **the business associate contract cannot authorize any uses or disclosures that the covered entity itself cannot make.** Therefore, **data mining by the business associate for any purpose not specified in the contract is a violation** of the contract and grounds for termination of the contract by the covered entity.”

(65 FR 82644)

# HIPAA and Online Tracking

## Tracking on **user-authenticated webpages**.

- Webpages that require users to log in before they are able to access webpage.
  - Likely involves PHI, e.g.,
    - **Individually identifiable info.**
      - E.g., name, phone, email address, IP address, MRIN, etc.
  - and
    - **Relates to past, present or future health, healthcare or payment for healthcare.**
      - E.g., appointments, sensitive medical info, prescriptions, billing, telehealth platform, patient portal, etc.

(OCR Guidance re Online Tracking)

# HIPAA and Online Tracking

## Tracking on **unauthenticated webpages**.

- Webpages that do not require users to log in before they are able to access webpage (e.g., main webpages re covered entity, addresses, visiting hours, etc.).
  - Likely do not implicate PHI because not sufficiently **related to person's healthcare**.
    - E.g., person visits provider's webpage to determine visiting hours, employment opportunities, student writing term paper.
  - But may implicate HIPAA if relates to the person's healthcare.
    - E.g., oncology patient looking for list of cardiology providers to obtain second opinion to treat brain tumor, etc.

(OCR Guidance re Online Tracking)

**But this is really untenable because it would require provider to know the person's intent in visiting the webpage!**

# HIPAA and Online Tracking

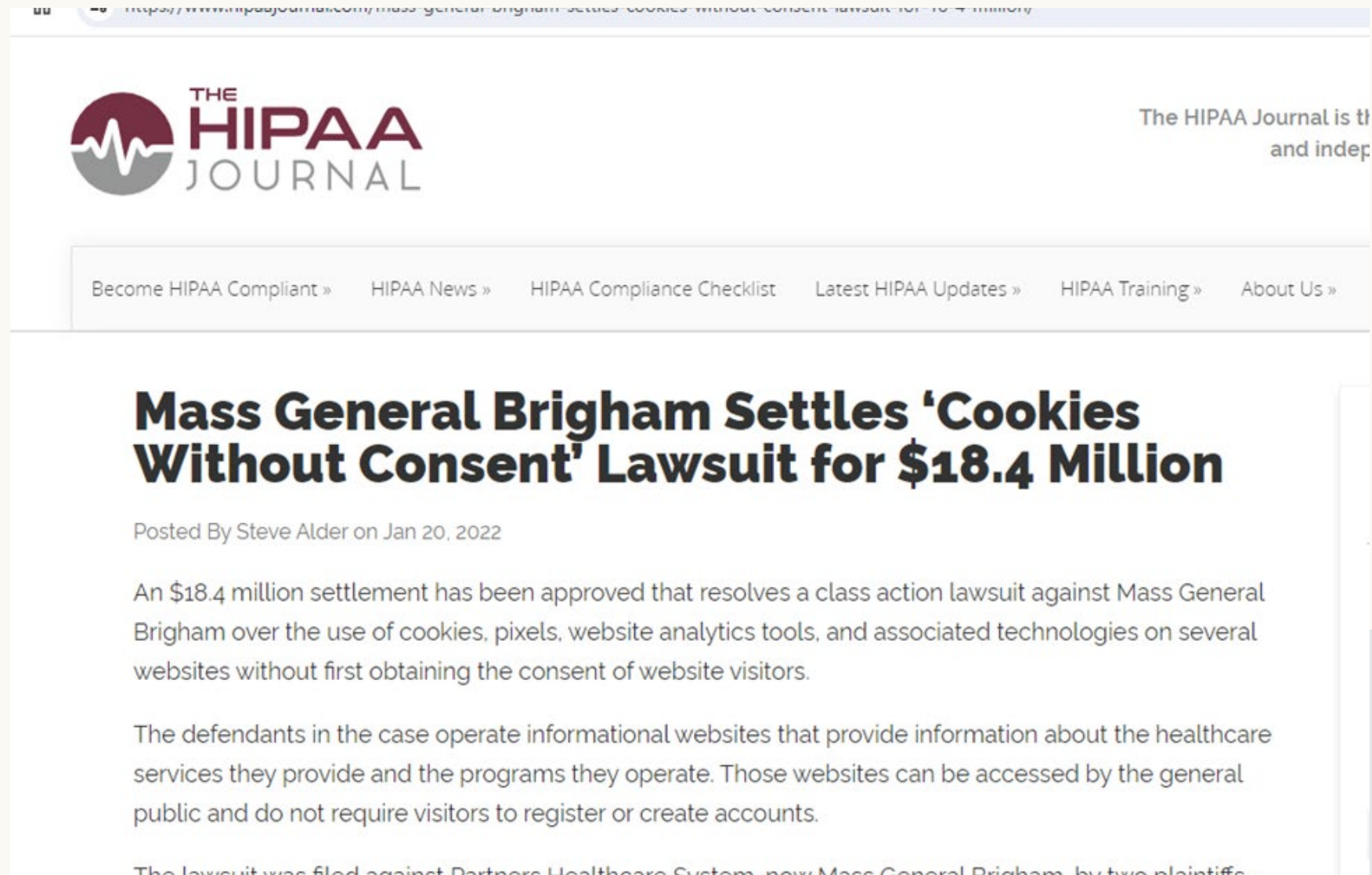
## Tracking on **mobile apps**.

- If app is provided by or on behalf of a covered entity, likely involves PHI, i.e.,
  - **Individually identifiable info**
    - E.g., user name, mobile number, IP address, device ID, etc.
  - and
  - **Relates to past, present or future health, healthcare or payment for care.**
    - E.g., tracks health condition, tracks treatment, pay bills, etc.
- If not developed or provided on behalf of a covered entity, then likely does not trigger HIPAA.
  - E.g., Apple Watch, smartphone apps, etc.
  - But FTC Act and FTC Health Breach Notification Rule (HBNR) may apply.

(OCR Guidance re Online Tracking)

# HIPAA and Online Tracking

- Beware private enforcement...



The screenshot shows a web browser displaying an article on 'The HIPAA Journal' website. The URL in the address bar is <https://www.hipaajournal.com/mass-general-brigham-settles-cookies-without-consent-lawsuit-for-18-4-million/>. The page features the journal's logo, a navigation menu with links like 'Become HIPAA Compliant', 'HIPAA News', and 'HIPAA Compliance Checklist', and a main article titled 'Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for \$18.4 Million'.

**THE HIPAA JOURNAL**

The HIPAA Journal is the  
and indep

[Become HIPAA Compliant »](#) [HIPAA News »](#) [HIPAA Compliance Checklist](#) [Latest HIPAA Updates »](#) [HIPAA Training »](#) [About Us »](#)

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

Posted By Steve Alder on Jan 20, 2022

An \$18.4 million settlement has been approved that resolves a class action lawsuit against Mass General Brigham over the use of cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.

The defendants in the case operate informational websites that provide information about the healthcare services they provide and the programs they operate. Those websites can be accessed by the general public and do not require visitors to register or create accounts.

The lawsuit was filed against Partners Healthcare System, now Mass General Brigham, by two plaintiffs

## Beware Private Lawsuits

- 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?

### Litigation Trends for 2023: Surge in Web Tracking Class Actions

by: John C. Cleary, Pavel (Pasha) A. Sternberg, Catherine A. Green, Elizabeth M. Marden, Elizabeth (Liz) Harding, and Colin H. Black of Polsinelli PC - *Intelligence*

© Posted On Wednesday, January 18, 2023



**RELATED PRACTICES & JURISDICTIONS**

Litigation Trial Practice

Communications Media Internet

All Federal

📄 📧 ⬇️ ⓘ

# HIPAA and Online Tracking

- ✓ Ensure uses of PHI collected from tracking technologies are for permissible purpose.
- ✓ Ensure disclosures to vendors are permitted by patient agreements and BAA.
- ✓ Comply with minimum necessary rule.
- ✓ Obtain patient's HIPAA-compliant authorization if necessary.
  - *General notice privacy policy or website terms and conditions is not sufficient!*
- ✓ Obtain BAA with vendors who may collect or receive PHI.
  - Specify permissible uses consistent with HIPAA rules.
  - May need to change vendors if they will not execute BAA.
  - BAA may allow vendor to de-identify PHI on behalf of covered entity but must be authorized in BAA.

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

# HIPAA and Online Tracking

- ✓ Comply with security rule when using or preventing tracking technologies.
  - “OCR is prioritizing compliance with the HIPAA Security Rule in investigations into the use of online tracking technologies.”
  - Include tracking technology in risk assessment.
  - Include required administrative, technical and physical safeguards (e.g., encrypting ePHI; enable appropriate authentication; access controls; audits; etc.).
- ✓ Notify patients and OCR of breaches per breach reporting rule.

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



# HIPAA and ePHI Transmissions

- 2/8/24: CMS revised memo allowing texting of patient orders for hospitals and CAHs. (QSO-24-05-Hospital/CAH)

But still subject to HIPAA:

- General rule: encryption is an addressable standard under the HIPAA rule. (45 CFR 164.312(e))
  - ✓ Secure personal devices such as smartphones.
  - ✓ Use secure (encrypted) platform to transmit e-PHI, including e-mail and text.
- Exception: patient has right to request communication by alternative means, including unsecure means. (45 CFR 164.522(b)).
  - ✓ Notify patient that communication may not be secure and obtain patient's consent to send by unsecure means. (<https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html>)

# HIPAA Reproductive Rights Rule



# HIPAA Reproductive Rights Rule

- Published 4/26/24
  - Goal: prevents state officials/regulators from getting info about patients to prosecute those who may cross the state line to obtain reproductive healthcare in another state where it is legal.
  - **Prohibition only applies if reproductive healthcare is legal, not illegal.**
- Effective Date: 6/25/24.
- Compliance Date:
  - Reproductive healthcare info provisions: **by 12/23/24.**
  - Notice of Privacy Practices: **by 2/16/26.**

(89 FR 2024)

# HIPAA Reproductive Rights Rule

- Applies to PHI re “reproductive health care”, i.e., “healthcare that that affects the heath of an individual in all matters relating to the reproductive system and to its functions and processes.”

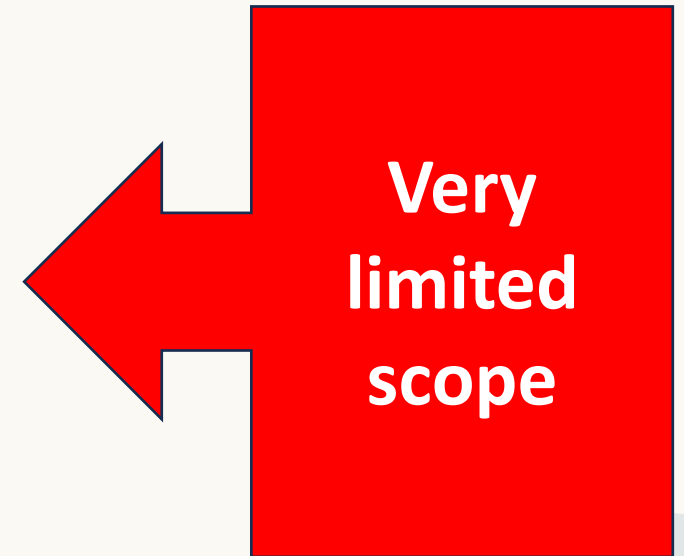
(45 CFR 160.103)

- If reproductive healthcare is legal, covered entities may not disclose reproductive healthcare PHI for purposes of criminal, civil or administrative liability or investigation.

(45 CFR 502(a)(5))

- Must obtain attestation from persons seeking reproductive healthcare PHI.

(45 CFR 509)



# Reproductive Rights Rule: Protection of Reproduction Care PHI

- 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.

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

- **But...**

# Reproductive Rights Rule: Protection of Reproduction Care PHI

Prohibition on use or disclosure of reproductive care PHI 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; 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.*

# Reproductive Rights Rule: Personal Representatives

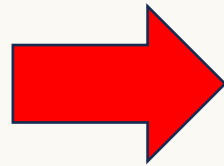
- “Personal representative” may generally access patient’s PHI.  
(45 CFR 164.504(g)(1))
- Notwithstanding any state law to the contrary, a covered entity may elect not to treat person as the personal representative if both the following apply:
  - Covered entity has reasonable belief that:
    - Patient 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))

# Reproductive Rights 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 Rights 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)).

✓ **OCR intends to publish a model attestation form.**

# Reproductive Rights Rule Webinar

- 6/20/24: HHS, OCR & ONC Joint Briefing on Reproductive Health Care Privacy.
- [https://capconcorp.zoom.us/webinar/register/WN\\_QI76yKQnT4Gki15Kf5p0og](https://capconcorp.zoom.us/webinar/register/WN_QI76yKQnT4Gki15Kf5p0og).



**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES**  
**Office for Civil Rights**

---

June 12, 2024

**Webinar: HHS OCR & ONC Joint Briefing on 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

# 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.”

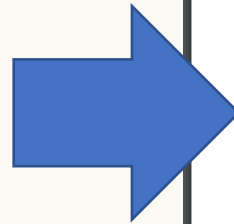
(45 CFR 164.512(f)(1)(C))

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

# HIPAA and Telehealth

- OCR has emphasized privacy and security in telehealth
- In 10/22, OCR published guidance concerning HIPAA concerns in audio-only telehealth.
- On 8/9/23, relaxed security standards for telehealth platforms ended.
- In 10/23, OCR published guidance for providers and patients concerning privacy and security risks in telehealth.

(<https://www.hhs.gov/hipaa/for-professionals/special-topics/telehealth/index.html>)



## Telehealth Privacy Tips for Providers



### What are the data privacy and security risks in telehealth?

- Privacy risk** is when an individual lacks control over the collection, use, and sharing of their health data.
- Security risk** is when there is unauthorized access to an individual's health data during the collection, transmission, or storage.
- These risks can affect trust between the patient and provider and contribute negatively to adherence and continuity of care.



### How do I fulfill privacy obligations during a telehealth session?

- Privacy and security risks** are present for in-person, remote monitoring, and virtual visits. Electronic transmission of data means greater privacy and security risks.
- Make sure you are up-to-date on security and protections requirements for [HIPAA compliance](#) and are aware of other [legal considerations](#).
- Providers have an **ethical obligation** to discuss privacy and security risks. These discussions can be part of a patient-centered care plan to help ensure confidentiality.



### How do I communicate privacy protections to patients?

- Make privacy part of the workflow by confirming identities of everyone present at each telehealth session and communicate how any third-parties may be involved.
- Set up and communicate the below safeguards to your patients:**
  - Create unique user identification numbers
  - Use password protected platforms
  - Establish automatic logoff



### How do I protect my own privacy and reduce risk of breaches?

- Health data breaches are costly and can involve investigations, notifying patients, and recovering data, so providers need to be familiar with their security features.
- Establish the below processes:**
  - Routinely review your telehealth privacy and security policies.
  - Schedule regular deletion of files on mobile devices.
  - Utilize data back-up and recovery processes in case of breach.
- Conduct a **security evaluation** from an independent party on your telehealth system to verify security features such as authentication, encryption, authorization, and data management.
- Check out more security [tips](#) from the Office of the National Coordinator for Health Information Technology.

# HIPAA

## Proposed Privacy Rule Changes

COMING  
SOON

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))

# 42 CFR Part 2 Rules

**SUBSTANCE USE  
DISORDER  
RECORDS**

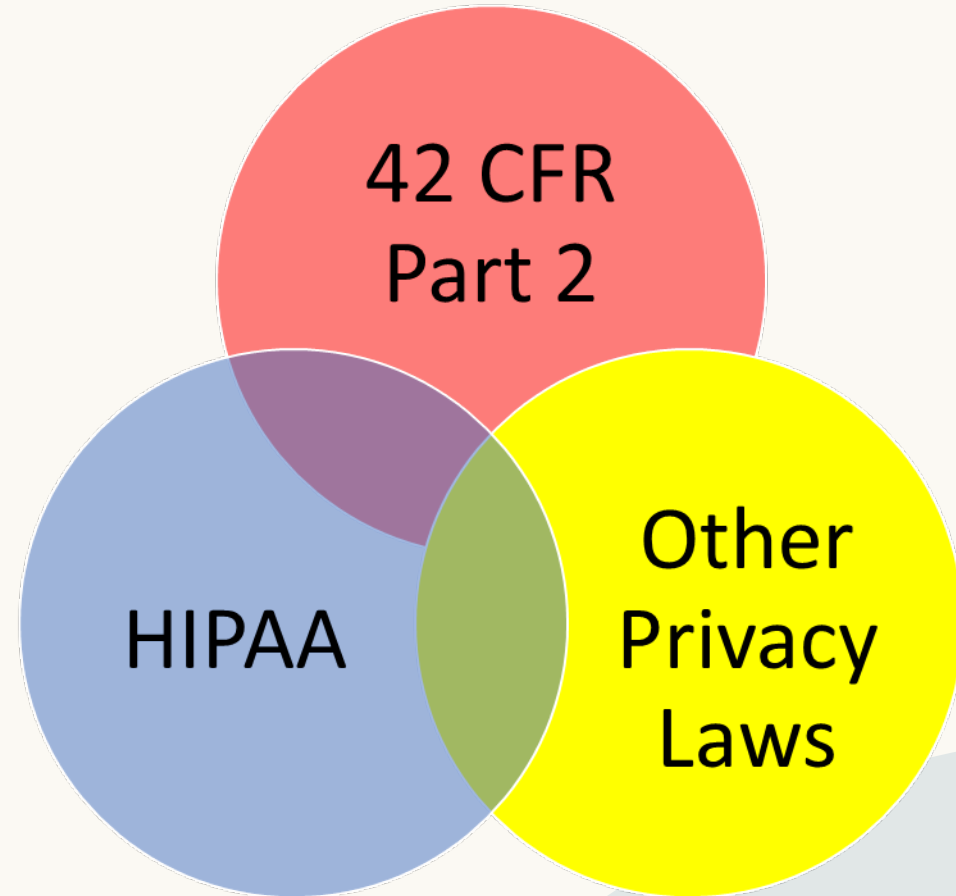


# Privacy Laws



Comply with the law that provides the most privacy protection, e.g.,

- HIPAA
- 42 CFR Part 2
- Other state or federal privacy rules



# 42 CFR Part 2 Final Rule

- Issued 2/8/24.
  - Effective 4/16/24.
  - **Enforced 2/16/26.**
- (89 FR 12472)



- Implements CARES Act 3221 (42 USC 290dd-2) to more closely align Part 2 with HIPAA.
  - HIPAA enforcement applies to Part 2.
    - OCR enforces Part 2 along with HIPAA.
    - HIPAA penalties replace criminal penalties.
    - Breach notification.
  - 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

- Applies to info that:
  - Identifies a patient as having, having had, or referred for a substance use disorder; and
  - Is created, received, or acquired by a federally assisted SUD program.
- Applies to:
  - Federally assisted SUD program.
  - Recipients of SUD info.
- Prohibits use or disclosure of SUD info unless:
  - Have patient consent, or
  - Fit within limited exception permitting disclosure.
- Must provide notice of Part 2 obligations to most recipients.
- Most recipients must comply with Part 2 obligations.

(42 CFR 2.11-2.13)

# Part 2 “Federally Assisted”

- “Federally assisted” =
  - Carried out under license or authorization granted by U.S. dept or agency (*e.g.*, participating in Medicare; DEA registration; or authorization to conduct maintenance treatment or withdrawal management).
  - Supported by funds provided by a U.S. department or agency (*e.g.*, receiving federal financial assistance, Medicaid, grants, etc., even if federal money does not pay directly for SUD services);
  - Program is tax-exempt or claims tax deductions relating to program; or
  - Conducted directly or by contract or otherwise by any dept or agency of the United States.
    - Special rules for VA or armed forces.

(42 CFR 2.12(b))

- Not purely private pay programs, but HIPAA likely applies.

# Part 2 “Program”

- “Program” =
  - Individual or entity (other than general medical facility\*) that holds itself out as providing and provides SUD diagnosis, treatment or referral.
  - Identified unit in a general medical facility\* that holds itself out as providing and provides SUD diagnosis, treatment or referral.
  - Medical personnel in a general medical facility\* whose primary function is providing SUD diagnosis, treatment or referral and who are identified as such providers.

(42 CFR 2.11; 2.12(e))

\* “General medical facilities” = hospitals, trauma centers, FQHCs, maybe primary care clinic.

(SAMHSA FAQ 10, <https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs>)

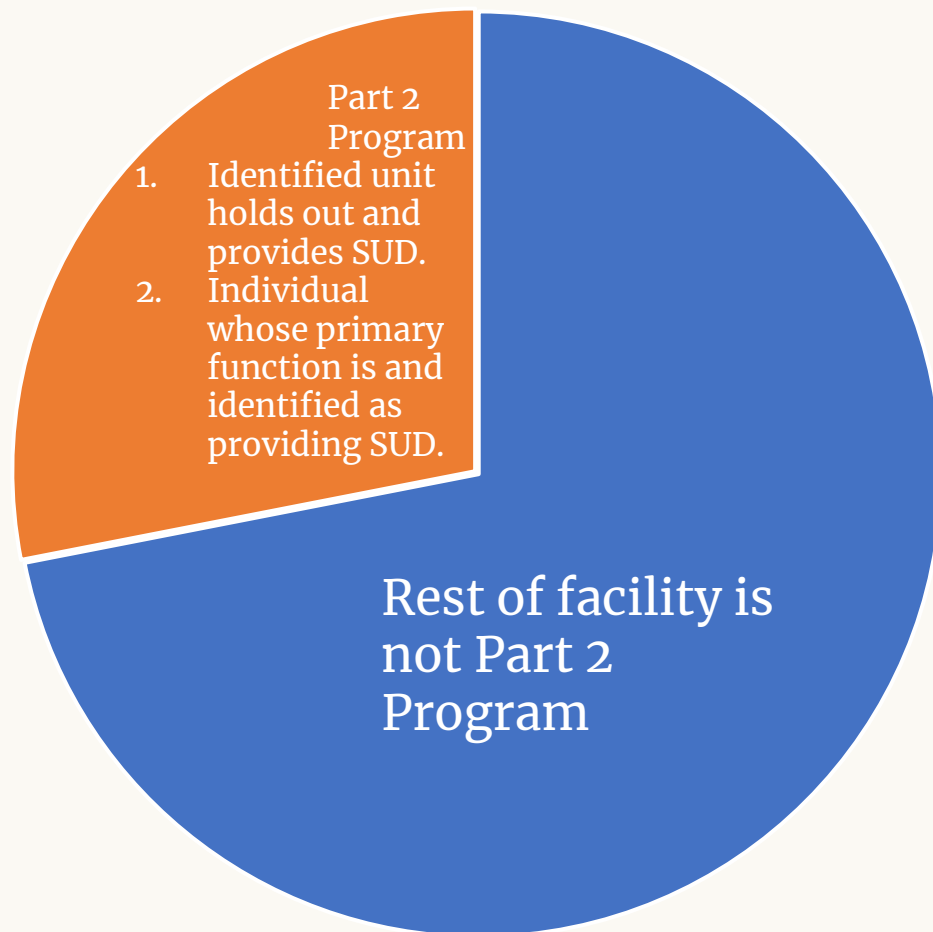
# Part 2

## Federally Assisted “Program”

Individual or Entity; <u>Not</u> General Medical Facility	General Medical Facility	
	Identified Unit	Medical Personnel or Staff
<ol style="list-style-type: none"> <li>1. Holds itself out as providing SUD diagnosis, treatment, or referral for treatment, <i>and</i></li> <li>2. Provides SUD diagnosis, treatment, or referral for treatment</li> </ol>	<ol style="list-style-type: none"> <li>1. Holds itself out as providing SUD diagnosis, treatment, or referral for treatment, <i>and</i></li> <li>2. Provides SUD diagnosis, treatment, or referral for treatment</li> </ol>	<ol style="list-style-type: none"> <li>1. Primary function is to provide SUD diagnosis, treatment or referral for treatment, <i>and</i></li> <li>2. Identified as such providers</li> </ol>

# Part 2 Federally Assisted Program

General Medical Facility



- Only the SUD unit/provider are the “program”.
- Program must comply with Part 2 in disclosing SUD info outside the program, *e.g.*,
  - Per consent
  - To administrative entity with control
  - To QSO
  - Other exception
- Program must have administrative controls in place to share SUD info.

# Recipients Subject to Confidentiality Restrictions

Confidentiality requirements apply to certain recipients of SUD info, *e.g.*,

- Entities with direct administrative control over Part 2 program.
- Qualified service organization (QSO).
  - Like HIPAA business associate.
  - Includes BAAs of Part 2 program if Part 2 program is covered by HIPAA.
- Lawful holder of SUD info, *i.e.*,
  - Received copy of patient's written consent + notice of Part 2 requirements, or
  - Received SUD info per exception to written consent requirement.
- Persons receiving SUD info from Part 2 program, covered entity, business associate, intermediary or lawful holder who are notified of prohibited redisclosure per 42 CFR 2.32.

(42 CFR 2.11 and 2.12(d))

# Disclosure of SUD Info

## WITH PATIENT'S CONSENT

- Consent for treatment, payment and operations: may obtain one consent for all such future uses.
- Other purposes: as specified in consent.
- ✓ Consent must contain required elements.
- ✓ Provide copy of consent + notice of Part 2 obligations with disclosure.

(42 CFR 2.31-2.33)

## WITHOUT PATIENT'S CONSENT

- Within Part 2 program if need to know.
  - Between Part 2 program and direct administrative control.
  - To QSO if have qualified service organization agreement (QSOA).
  - Report to law enforcement re crime on premises or threat against program personnel.
  - Report suspected child abuse or neglect.
- (42 CFR 2.12(c))
- Disclosure of de-identified info for public health purposes.
  - Medical emergency.
  - Scientific research subject to conditions.
  - Audits and investigations subject to conditions.
  - Per compliant order + subpoena.

(42 CFR 2.51-2.67)

# Disclosure with Consent: Copy of Consent + Notice

May use either of the following 2 permissible statements:

1. “This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, **the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies:**  
(i) Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2.  
(ii) You are a covered entity or business associate and have received the record for treatment, payment, or health care operations, or  
(iii) You have received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E. A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31).”
2. “42 CFR part 2 prohibits unauthorized use or disclosure of these records.”  
(42 CFR 2.32(a))



# Redisclosure of SUD Info

- If received disclosure per consent, Part 2 limits recipients' use or redisclosure of SUD info.
- Authority to redisclose depends on:
  - Scope of consent, e.g.,
    - Specific limitations, and
    - For treatment, payment or healthcare operations.
  - Whether recipient is a HIPAA-covered entity or business associate.
    - Covered entities and business associates may generally redisclose as permitted by HIPAA.
  - Purpose of the use or redisclosure.
  - Entity to whom the redisclosure is made.

(42 CFR 2.33)

✓ *Check consent and notice of redisclosure accompanying consent.*

# Part 2

## Patient Rights

- Patient not required to consent to uses or disclosures for TPO.
- Patient may withdraw consent or restrict disclosures for TPO.
- Patient may receive accounting of disclosures, including \*disclosures for TPO if maintain electronic health record.
  - \*Tolled until HIPAA rule implementing this requirement is issued.
- Program must have complaint process.
- Patient may file complaint with OCR as with HIPAA.
- Program may not intimidate, threaten, or retaliate in response to patient exercising Part 2 rights.
- Program must post and provide Notice of Confidentiality Protections.

(42 CFR 2.24)

# Part 2 Notice to Patient

Upon admission or when patient gains capacity, Part 2 program must:

- Inform patient that federal law protects confidentiality of SUD info.
- Give patient written notice of the program's duties and privacy practices as specified in the regulations.
  - Required header and statements
  - Required elements

(42 CFR 2.22)

- *HHS plans to modify HIPAA requirements for notice of privacy practices to align with part 2 notice requirements.*



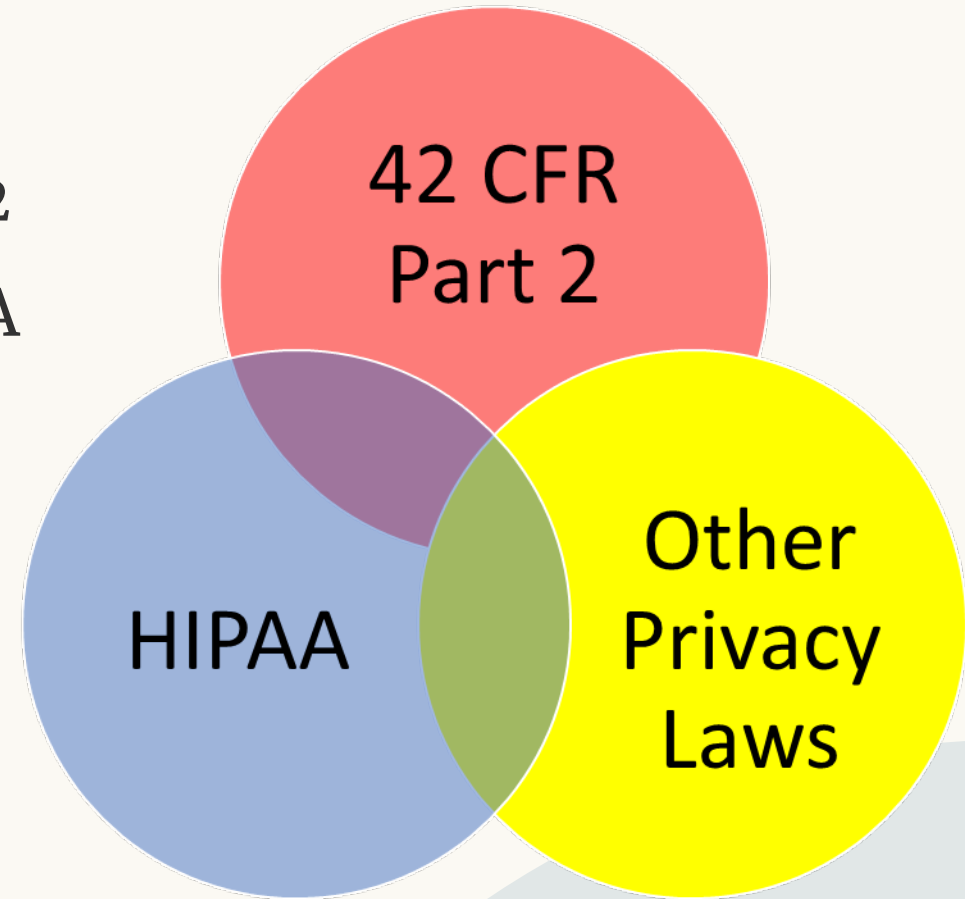
# Part 2 Security

- Part 2 programs and lawful holders must have formal policies and procedures to protect against unauthorized use or disclosure of SUD info or threats to security of SUD info.
- Policies and procedures must address all of the following for paper and e-info:
  - Transfer and removing records.
  - Destroying records, including sanitizing media.
  - Maintaining records in secure room, cabinets or facilities.
  - Using and accessing workstations, rooms, cabinets or facilities.
  - De-identifying records consistent with HIPAA standards at 45 CFR 164.514(b).
- **These standards do not apply to family, friends, and other informal caregivers who are lawful holders.**

(42 CFR 2.16)

# Part 2 and HIPAA

- ✓ Remember: if you are a covered entity or business associate as well as a Part 2 program, you must comply with HIPAA in addition to the Part 2 rules....



# OCR/SAMHSA Webinar

<https://www.youtube.com/watch?v=F3ZZgCXpT4k>

## OCR and SAMHSA Release Webinar on the New Final Rule Modifying the Confidentiality Provisions for Substance Use Disorder Patient Records



OCR HIPAA Security Rule information distribution <OCR-SECURITY-LIST@LIST.NIH.GOV> on behalf of OS OCR SecurityList, OCR (HHS/OS) <OCRSecurityList@HHS  
To OCR-SECURITY-LIST@LIST.NIH.GOV

Retention Policy | Inbox 120 Days - Remove Items (4 months)

Expires 8/14/2024



Tue 4/16/2024 2:12



### **U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES Office for Civil Rights**

**April 16, 2024**

### **OCR and SAMHSA Release Webinar on the New Final Rule Modifying the Confidentiality Provisions for Substance Use Disorder Patient Records**

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the Substance Abuse and Mental Health Services Administration (SAMHSA) release a webinar recording on the new finalized modifications to the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations at 42 CFR Part 2 ("Part 2"), which protect the privacy of patients' SUD treatment records.

The new Part 2 Final Rule increases coordination among providers treating patients for SUDs, strengthens patient confidentiality protections through civil enforcement, and enhances integration of behavioral health information with other medical records to improve patient health outcomes.

<https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs>

 An official website of the United States government [Here's how you know](#) ▾

 **In Crisis? Call or Text 988** >>



[Home](#) | [Site Map](#) | [Contact Us](#)

Search SAMHSA.gov

Search

[Find Help](#) | [Practitioner Training](#) | [Public Messages](#) | [Grants](#) | [Data](#) | [Programs](#) | [Newsroom](#) | [About Us](#) | [Publications](#)

[Home](#) » [About Us](#) » [Who We Are](#) » [Laws and Regulations](#) » Confidentiality Regulations FAQs



About Us

Who We Are

Leadership

Regional Offices

Offices and Centers

Laws and Regulations

**Confidentiality Regulations FAQs**

Listening Session Comments on Substance Abuse Treatment Confidentiality Regulations

Olmstead v. L.C. Resources

Data Strategy

## Substance Use Confidentiality Regulations

The [Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? \(PDF | 1.6 MB\)](#) fact sheet describes how 42 CFR Part 2 applies to the electronic exchange of healthcare records with a Part 2 Program.

### Applying the Substance Use Confidentiality Regulations

Substance Abuse and Mental Health Services Administration  
U.S. Department of Health and Human Services  
42 CFR Part 2 (REVISED)

In 2010, the HHS Substance Abuse and Mental Health Services Administration (SAMHSA) and the HHS Office of the National Coordinator (ONC) published FAQs “Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE).” The 2010 FAQs are available at [Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange \(HIE\) \(PDF | 381 KB\)](#).

*These Frequently Asked Questions (FAQs) are for information purposes only and are not intended as legal advice.*

<https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-part-2/index.html>



U.S. Department of  
**Health and Human Services**

Enhancing the health and well-being of all Americans

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

## Health Information Privacy



[HIPAA for Individuals](#)

[Filing a Complaint](#)

[HIPAA for Professionals](#)

[Newsroom](#)

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Special Topics](#) > HIPAA and Part 2

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +



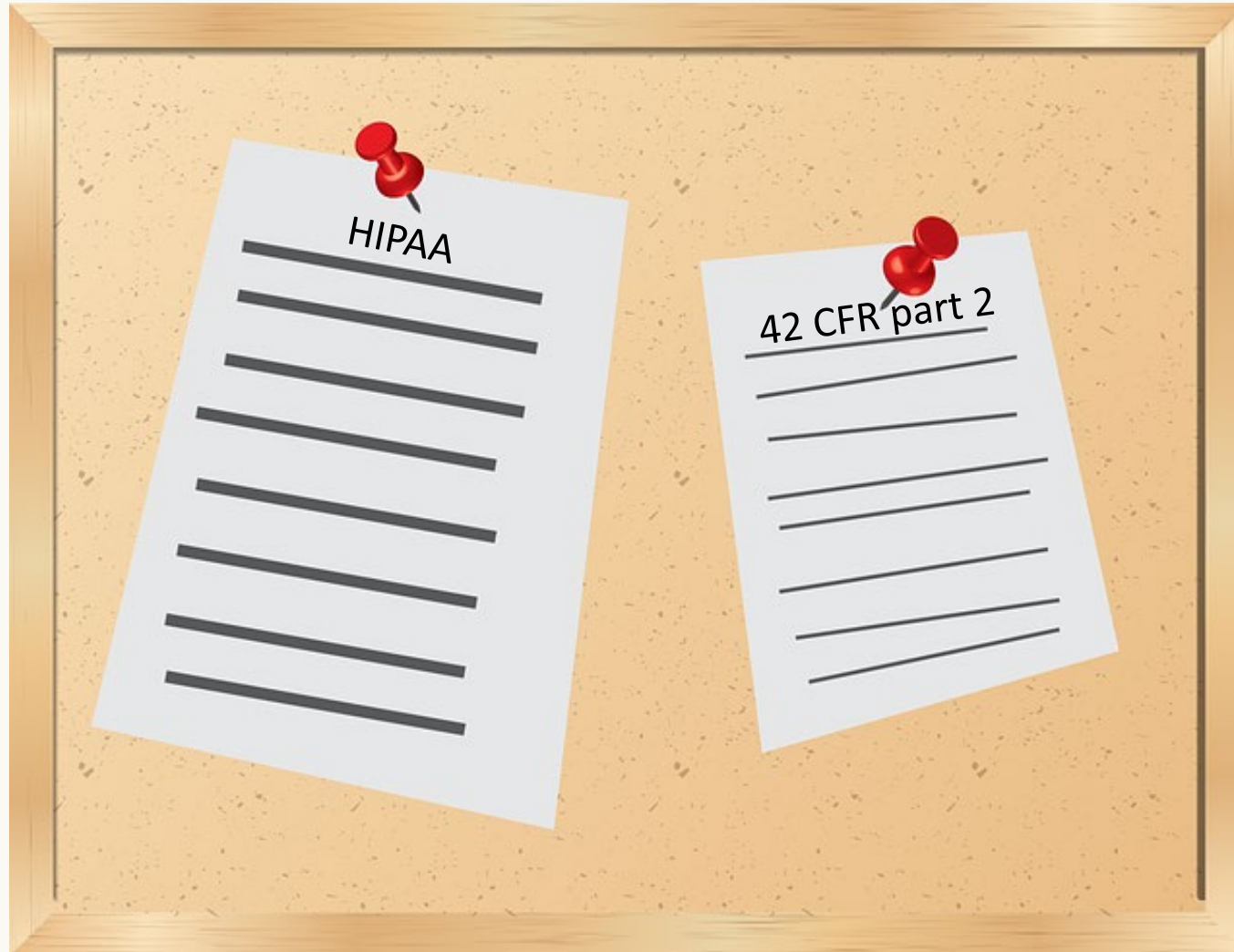
## HIPAA and Part 2

On November 28, 2022, the U.S. Department of Health & Human Services, through the Office for Civil Rights (OCR) in coordination with the Substance Abuse and Mental Health Services Administration (SAMHSA), issued a Notice of

art



# HIPAA Notice of Privacy Practices



# HIPAA: Notice of Privacy Practices

- Reproductive Right Rule modified NPP requirements to accommodate Part 2 changes.
  - Covered entities creating or maintaining SUD records subject to Part 2 must provide the notice to the patient as required by 42 CFR 2.22.
    - Uses and disclosures.
    - Patient rights.
    - Covered entities' duties.
- (45 CFR 164.520(a)(2))
- Other covered entities must update their NPP.
- Must comply by **2/16/26**.
- ✓ *Check applicable regulations when drafting updated NPP.*

# NPP Requirements

- Required header: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
- Description + example of uses and disclosure for treatment, payment and health care operations.
- Description of each use or disclosure not requiring patient authorization.
- Incorporate limits of more stringent laws, **including 42 CFR part 2.**
- **Description + example of uses and disclosures of reproductive PHI prohibited by 45 CFR 164.502(a)(5)(iii), e.g., for criminal, civil or administrative liability.**
- **Description + example of uses and disclosures for which attestation is required under 45 CFR 164.509.**
- **Statement that information disclosed per HIPAA may be subject to redisclosure by recipient and no longer protected.**

(45 CFR 164.520(b)(1)(i)-(ii))

# NPP Requirements

- If covered entity intends to engage in certain activities, must include statement notifying patient:
  - Fundraising.
  - **SUD records received from Part 2 program may not be sued or disclosed in civil, criminal, admin or legislative proceedings against patient without patient's consent or Part 2 court order.**
  - **If Part 2 program uses info for fundraising, patient must be given opportunity to opt out.**

(45 CFR 164.520(b)(1)(iii))

# NPP Requirements

- Describe patient rights and how they may be exercised
  - Request restrictions on use or disclosure for treatment, payment and operations and exceptions per 164.522(a).
  - Receive PHI by confidential communications per 164.522(b).
  - Inspect and copy PHI per 164.524.
  - Amend PHI per 164.526.
  - Receive accounting of PHI per 164.528.
  - Receive paper copy of NPP upon request.

(45 CFR 164.520(b)(1)(iv))

# NPP Requirements

- Describe covered entity's duties.
  - Required by law to maintain privacy of PHI, provide notice of its duties and privacy practices with ~~respect to PHI~~, and notify patient of breaches of unsecured PHI.
  - Comply with NPP in effect.
  - To apply change in its NPP to records created before change, reserve right to do so.
- Explain right to complaint to covered entity and HHS.
- Include contact info of person to contact if have additional questions.
- Effective date.

(45 CFR 164.520(b)(1)(iv))

# NPP Revisions

- Covered entity must promptly revise and distribute its NPP whenever there is a material change to
  - the uses or disclosures,
  - the individual's rights,
  - the covered entity's legal duties, or
  - other privacy practices stated in the NPP.

(45 CFR 164.520(b)(3))

- Post new NPP on website and in facility.
- Make new NPP available upon request.
- If using joint notice, ensure joint notice complies by deadline.

(45 CFR 164.520(c)-(d))

- ✓ *OCR intends to publish a model Notice of Privacy practices.*
- ✓ *Watch for additional changes if the proposed HIPAA rule is finalized*

# NPP and Privacy Policy, Terms and Conditions



- Many websites or apps include privacy policies and/or terms and conditions.
  - State law requirements.
  - Industry standards.
- Ensure your general privacy policies, terms and conditions are consistent with your HIPAA Notice of Privacy Practices.
  - e.g., uses and disclosure of PHI for tracking, marketing, etc.
  - Elements and form required by HIPAA.
- ✓ HIPAA covered entities must comply with HIPAA and NPP.
- ✓ Business associates may need to comply with covered entity clients' NPP to the extent disclosures contrary to NPP would not be permitted by covered entity and, therefore, by business associate.



# Expanded Govt Focus on Privacy



# FTC Enforcement

<https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach>



**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

[Enforcement](#) ▾ [Policy](#) ▾ [Advice and Guidance](#) ▾ [News and Events](#) ▾ [About](#)

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

## Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule

**Tags:** [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#) | [Health Privacy](#)

Does your business collect, use, or share consumer health information? When it comes to privacy and

# 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> )

- [Monument, Inc., U.S. v.](#) (June 7, 2024 )
- [Facebook, Inc., In the Matter of](#) (June 7, 2024 )
- [Blackbaud, Inc.](#) (May 20, 2024 )
- [InMarket Media, LLC](#) (May 1, 2024 )
- [Ring, LLC](#) (April 23, 2024 )
- [Cerebral, Inc. and Kyle Robertson, U.S. v.](#) (April 15, 2024 )
- [X-Mode Social, Inc.](#) (April 11, 2024 )
- [Rite Aid Corporation, FTC v.](#) (March 8, 2024 )
- [Global Tel Link Corporation](#) (February 23, 2024 )
- [Avast](#) (February 22, 2024 )
- [FTC v Kochava, Inc.](#) (February 5, 2024 )
- [Epic Games, In the Matter of](#) (January 10, 2024 )
- [CafePress, In the Matter of](#) (January 10, 2024 )
- [TruthFinder, LLC, FTC v.](#) (October 11, 2023 )
- [1Health.io/Vitagene, In the Matter of](#) (September 7, 2023 )
- [Edmodo, LLC, U.S. v.](#) (August 28, 2023 )
- [Vivint Smart Home, Inc.](#) (August 23, 2023 )
- [Amazon.com \(Alexa\), U.S. v.](#) (July 21, 2023 )
- [BetterHelp, Inc., In the Matter of](#) (July 14, 2023 )
- [Easy Healthcare Corporation, U.S. v.](#) (June 26, 2023 )



ABOUT THE FTC

NEWS & EVENTS

ENFORCEMENT

POLICY

TIPS & ADVICE

I WOULD LIKE TO...

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 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

“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 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 Health Breach Notification Rule (HBNR)

- Applies to vendors of personal health info, e.g., entities that collect health info on behalf of subject person.
  - Not entities covered by HIPAA (covered entities and business associates)
- Requires vendors of personal health provide notice following a breach involving unsecured information.
  - To consumers.
  - To FTC.
- Requires vendor service providers to notify vendor so they can notify consumers.
- If breach involves 500+ persons, must notify media.

(16 CFR part 316)

- **GoodRx pays \$1,500,000 for failing to report unauthorized disclosure of consumer health data to Facebook, Google, and others.**
- **Easy Healthcare (Premom ovulation tracking app) shared info with third parties, including AppsFlyer and Google.**

<https://www.ftc.gov/legal-library/browse/statement-commission-breaches-health-apps-other-connected-devices>



FEDERAL TRADE COMMISSION  
PROTECTING AMERICA'S CONSUMERS

[Enforcement](#) ▾ [Policy](#) ▾ [Advice and Guidance](#) ▾ [News and Events](#) ▾ [About the FTC](#) ▾ [Q](#)

[Home](#) / [Legal Library](#) / [Browse](#)

# Statement of the Commission on Breaches by Health Apps and Other Connected Devices



**Tags:** [Consumer Protection](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Health Privacy](#)

**Date:** September 15, 2021

**Matter Number:** P205405

**By:** [Federal Trade Commission \(FTC\)](#)

## Related Releases

[FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule](#)

## Related Events

# FTC Health Breach Notification Rule (HBNR)

- 4/26/24: FTC issues final update to HBNR.
  - Confirms HBNR application to health apps and similar technologies not covered by HIPAA.
  - Extends rule to entities that offer products and services through online services, including mobile apps, of vendors of personal health records.
  - “Breach of security” includes unauthorized acquisition of identifiable health info that occurs through data security breach or unauthorized disclosure.
  - Modifies required content of notice of breach.
- Effective **7/29/24**.

(89 FR 47028)

# SEC Cybersecurity Rules for Publicly Traded Entities

SEC regulations require publicly traded entities to report:

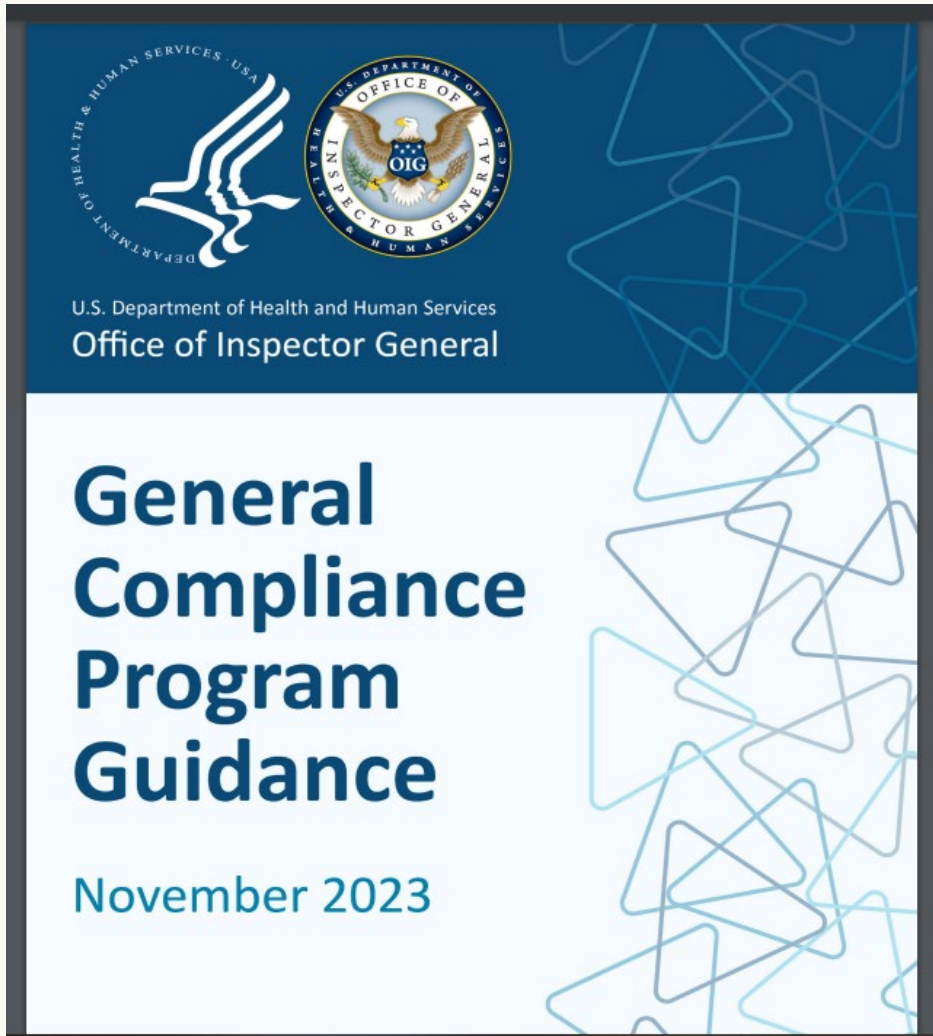
- Material cybersecurity incidents within four days, and
- Material information about regarding cybersecurity management.

(<https://www.sec.gov/news/press-release/2023-139>)

The screenshot shows the SEC website's press release page for Rule 2023-139. The header includes the SEC logo, the text "U.S. SECURITIES AND EXCHANGE COMMISSION", a search bar, and a "COMPANY FILINGS" link. A dark blue navigation bar contains links for "ABOUT", "DIVISIONS & OFFICES", "ENFORCEMENT", "REGULATION", "EDUCATION", "FILINGS", and "NEWS". On the left, a sidebar menu lists "Newsroom", "Press Releases", "Speeches and Statements", "SEC Stories", "Securities Topics", "Media Kit", "Press Contacts", "Events", "Webcasts", "Media Gallery", and "RSS Feeds". The main content area features a "Press Release" title with social media icons, followed by the headline "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies". Below the headline is the text "FOR IMMEDIATE RELEASE 2023-139" and the date "Washington D.C., July 26, 2023". The body text states that the SEC adopted rules requiring registrants to disclose material cybersecurity incidents and material information regarding their cybersecurity risk management, strategy, and governance. A quote from SEC Chair Gary Gensler is included, stating that the rules will benefit investors, companies, and the markets connecting them. To the right of the main text is a "Related Materials" section with links to "Final Rule" and "Fact Sheet".



# OIG General Compliance Program Guidance

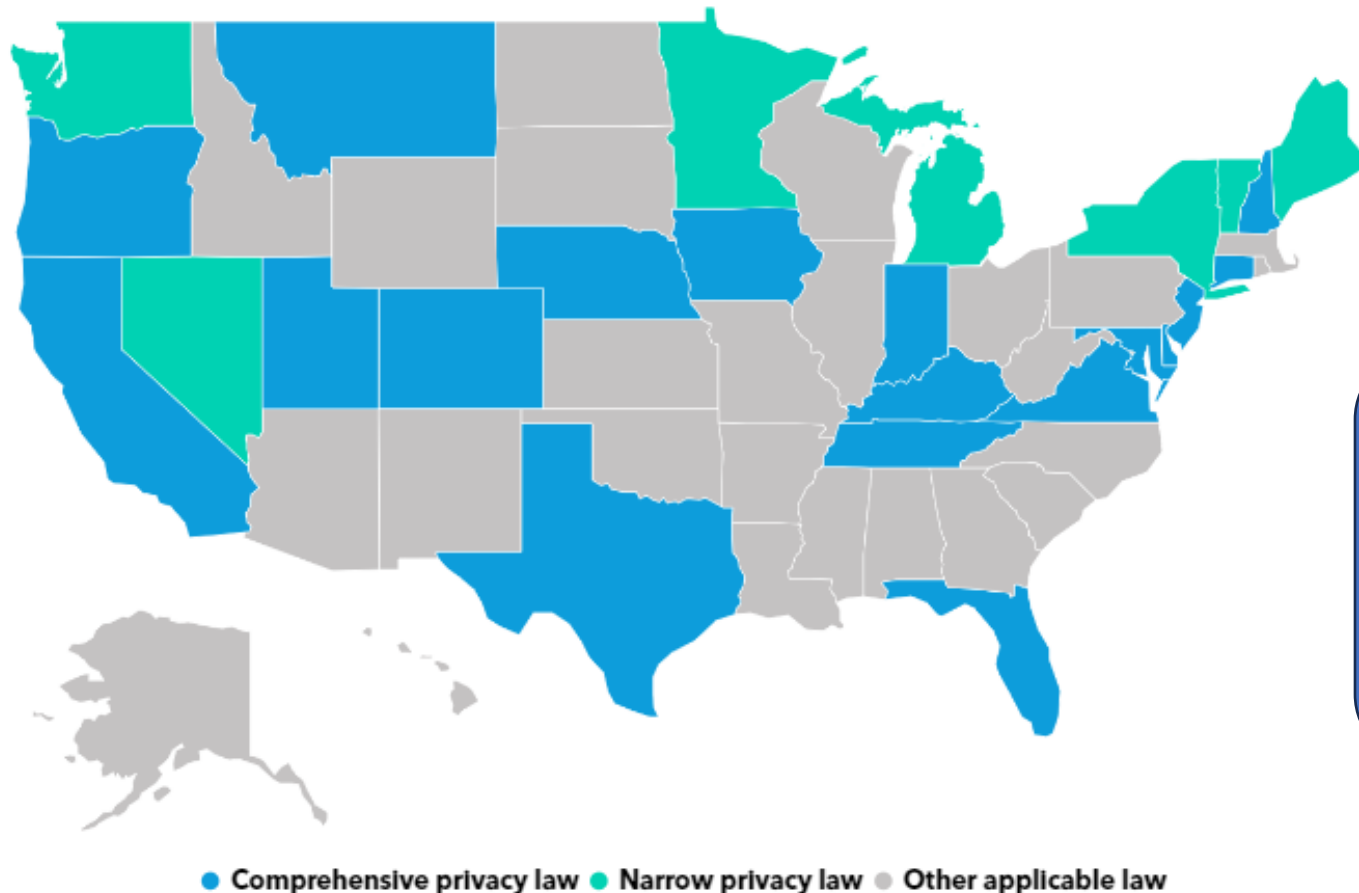


- “With increasing numbers of cybersecurity attacks aimed at HIPAA-regulated entities of all sizes, compliance with Privacy, Security, and Breach Notification Rule requirements should be a top compliance priority and included in all risk assessments.”

(<https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf#page=10>)

# State Data Privacy Laws

## U.S. states with consumer data privacy laws



Source: Bloomberg Law,  
<https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#row-66725b4d4cdd5>

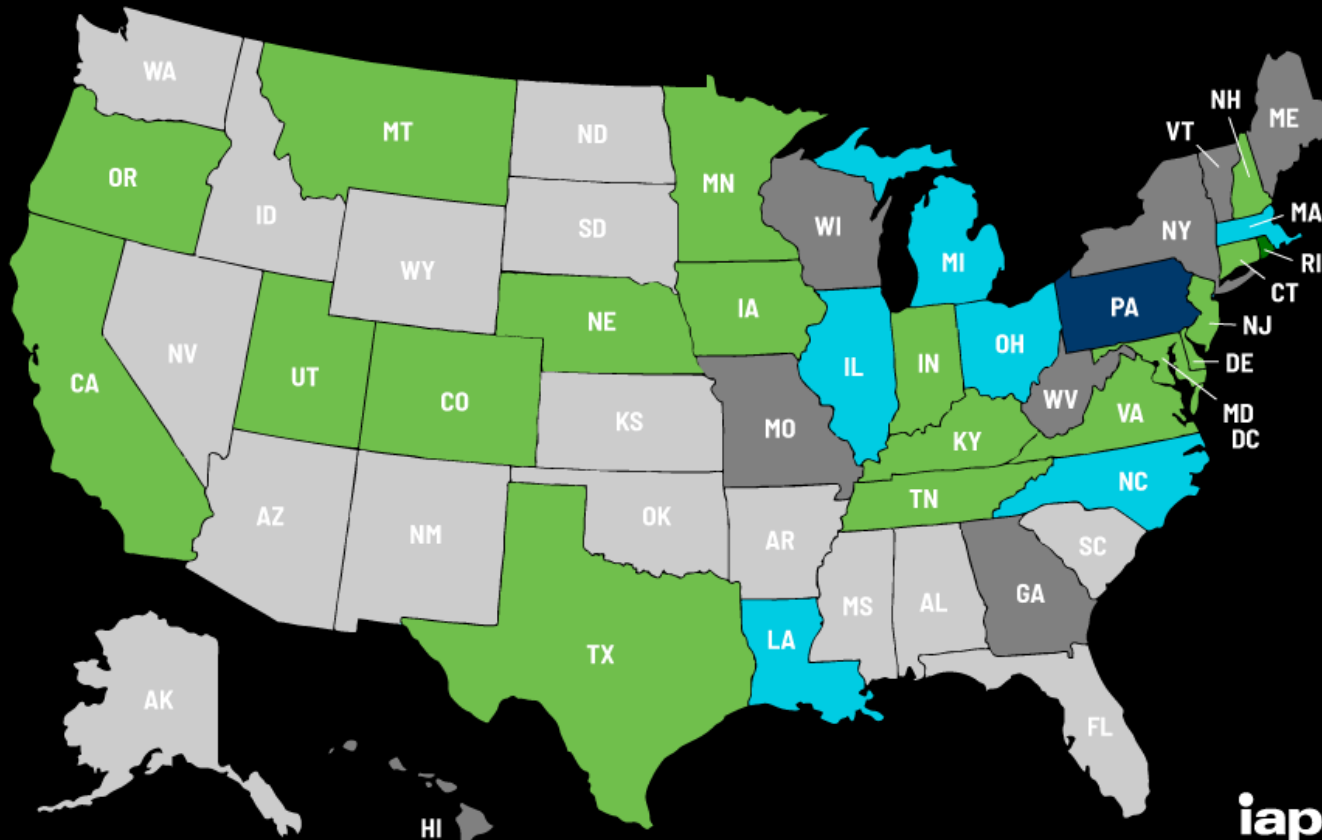
**Remember:**  
HIPAA requires you to comply with more restrictive law, including state laws.

# State Data Privacy Laws in Legislative Process

## US State Privacy Legislation Tracker 2024

### Statute/bill in legislative process

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bills introduced



Last updated 17 June 2024

iapp

Source:  
International Ass'n  
of Privacy  
Professionals,  
<https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>

# Cybersecurity



# Cybersecurity

## Cyberattack on Change Healthcare brings turmoil to healthcare operations nationwide

June 4 update: Federal regulators have provided updated guidance pertaining to breach notifications.



Nick Hut

Like 35 | 1

### Change Healthcare cyberattack fallout continues

Change Healthcare, part of Optum, suffered a cyberattack in late February.

#### Resources

[A list of payer contact:](#)

### HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack

Today, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a "Dear Colleague" letter addressing the cybersecurity incident impacting Change Healthcare, a unit of UnitedHealthcare Group (UHG), and many other health care entities. The cyberattack is disrupting health care and billing information operations nationwide and poses a direct threat to critically needed patient care and essential operations of the health care industry.

OCR enforces the [HIPAA Privacy, Security, and Breach Notification Rules](#), which sets forth the requirements that



World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Breakingviews ▾ Technology ▾ Investigations ▾ More

### Lawsuits over Change Healthcare data breach centralized in Minnesota

By **Brendan Pierson**

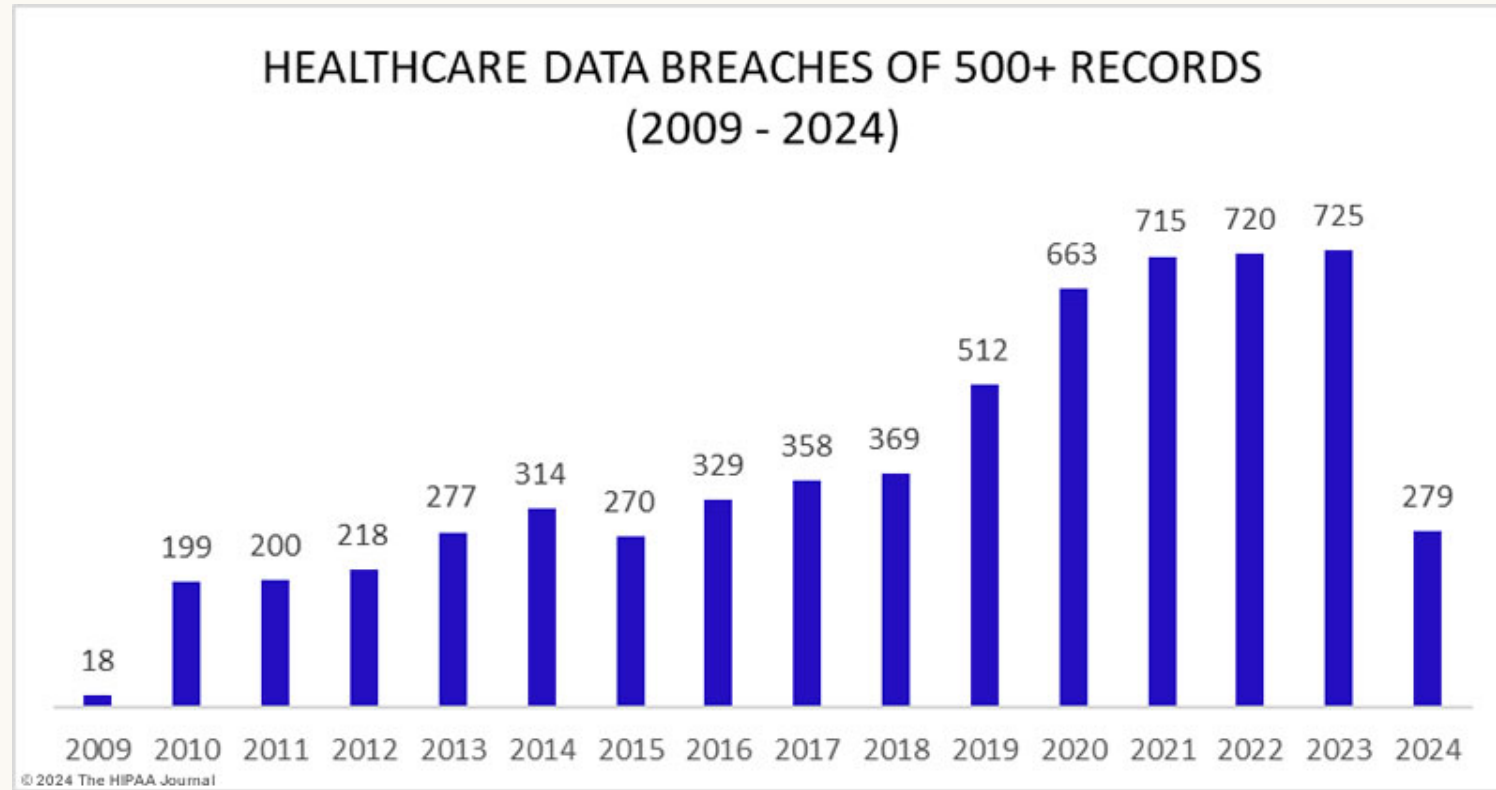
June 7, 2024 2:18 PM MDT · Updated a day ago



# Cybersecurity

According to HHS:

- 2018-22: 93% increase in large breaches
- 2018-22: 278% increase in large breaches from ransomware.
- 2023: 77% of large breaches resulted from hacking.
- 2023: Persons affected by large breaches increased 60% to 80,000,000.



Source: The HIPAA Journal

<https://www.hipaajournal.com/healthcare-data-breach-statistics/>

Consider impact on:

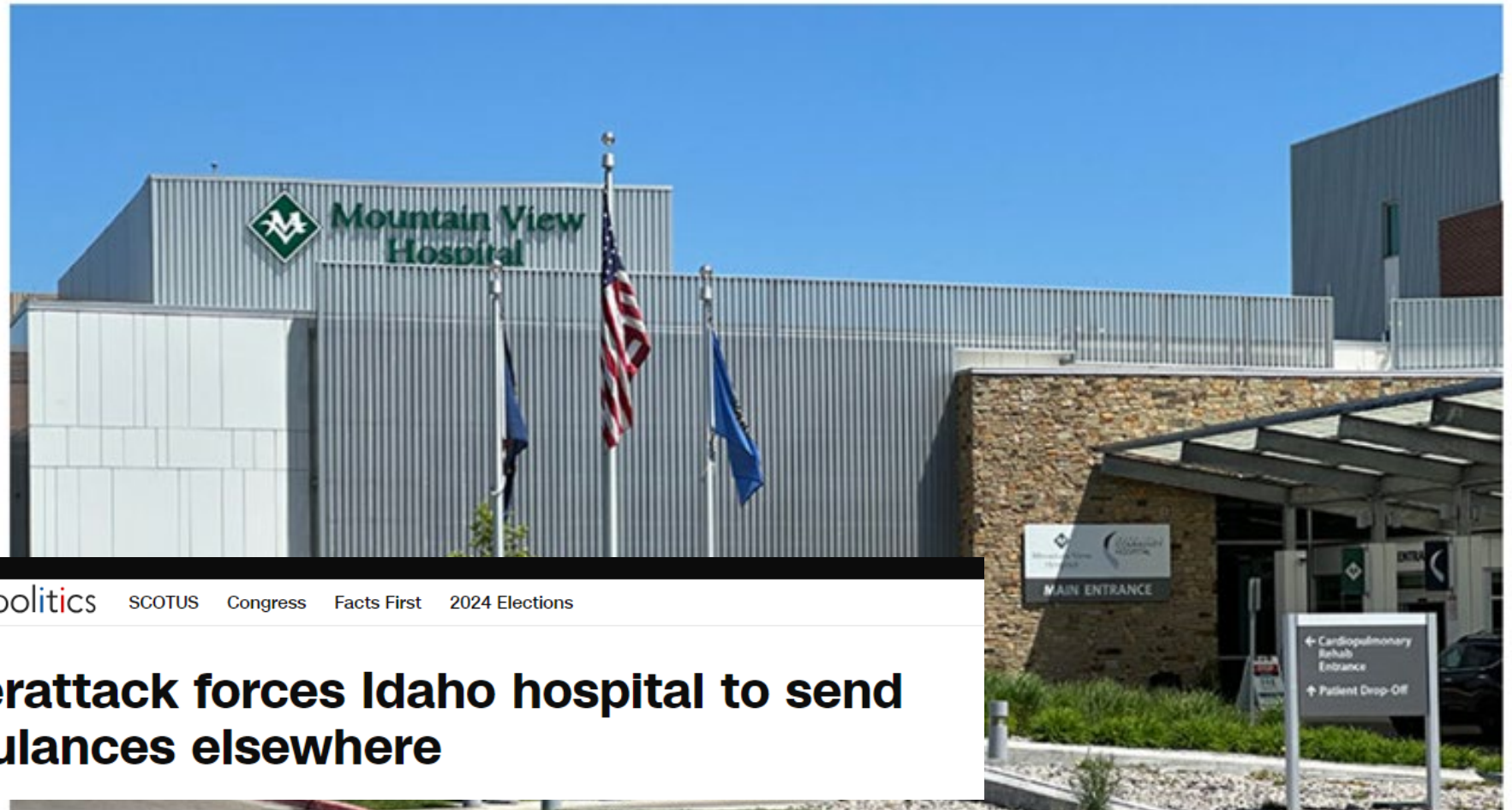
- Patient safety.
- Ability to function without data or with compromised data.
- Inability to bill.
- Damage to IT infrastructure.
- FTC or state law violations.
- Lawsuits.
- Bad press.

## Cyberattack on Mountain View Hospital still ongoing after two weeks

Published at 9:00 am, June 10, 2023 | Updated at 9:13 am, June 10, 2023



Logan Ramsey, EastIdahoNews.com



☰ CNN politics SCOTUS Congress Facts First 2024 Elections

## Cyberattack forces Idaho hospital to send ambulances elsewhere

# HHS Strategy Paper

<https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf>

## HEALTHCARE SECTOR CYBERSECURITY

Introduction to the Strategy  
of the U.S. Department of Health  
and Human Services



Coming 2024

On 12/6/23, HHS published strategy for strengthening cybersecurity for healthcare industry.

1. Establish voluntary cybersecurity performance goals.
2. Provide resources to incentivize and implement cybersecurity practices.
3. **Greater enforcement and accountability.**
  - **Cybersecurity requirements for hospitals through Medicare/Medicaid.**
  - **Update HIPAA Security Rule to include new cybersecurity rule requirements.**
  - **Increase civil penalties.**
  - **Increase resources for audits and investigation.**
4. HHS to provide one-stop shop for healthcare cybersecurity resources.



# HIPAA Penalties for Cybersecurity Lapses

“Our settlement highlights how ransomware attacks are increasingly common and targeting the health care system. This leaves hospitals and their patients vulnerable to data and security breaches... In this ever-evolving space, it is critical that our health care system take steps to identify and address cybersecurity vulnerabilities along with proactively and regularly review risks, records, and update policies. These practices should happen regularly across an enterprise to prevent future attacks.”

– – OCR Director Melanie Fontes

FOR IMMEDIATE RELEASE

October 31, 2023

Contact: HHS Press Office

202-690-6343

[media@hhs.gov](mailto:media@hhs.gov)

## HHS’ Office for Civil Rights Settles Ransomware Cyber-Attack Investigation

*OCR Settles with Business Associate in attack affecting over 200,000 individuals*

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a settlement under the Health Insurance Portability and Accountability Act (HIPAA) with Doctors’ Management Services, a Massachusetts medical management company that provides a variety of services, including medical billing and payor credentialing. The HIPAA Privacy, Security, and Breach Notification requirements that HIPAA-regulated entities must follow to protect the protected health information of 206,695 individuals. Ransomware is a type of malware designed to deny access to a user’s data, usually by encrypting the data. The attacker deployed the malware, until a ransom is paid. This marks the first ransomware settlement under HIPAA.

During Cybersecurity Awareness Month, and OCR has been working with entities covered by HIPAA to ensure better data security. Ransomware is a growing threat in health care. In the past four years, there has been a 239% increase in ransomware attacks involving hacking and a 278% increase in ransomware. This trend continues to be a concern. 77% of the large breaches reported to OCR. Additionally, the large breaches affected over 1 million individuals, a 60% increase from last year.

“Our settlement highlights how ransomware attacks are increasingly common and targeting the health care system.

**Paid \$80,000  
as a result of  
ransomware  
attack.**

# HIPAA: Penalties for Cybersecurity Lapses

FOR IMMEDIATE RELEASE  
February 2, 2023

Contact: HHS Press Office  
202-690-6343  
[media@hhs.gov](mailto:media@hhs.gov)

## HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking

*Banner Health pays \$1.25 million to settle cybersecurity breach that affected nearly 3 million people*

Today, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement with Banner Health Affiliated Covered Entities ("Banner Health"), a nonprofit health system headquartered in Phoenix, Arizona, to resolve a data breach resulting from a hacking incident by a threat actor in 2016 which disclosed the protected health information of 2.81 million consumers. The settlement is regarding the Health Insurance Portability and Accountability Act (HIPAA) Security Rule which works to help protect health information and data from cybersecurity attacks. The potential violations specifically include: the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization, insufficient monitoring of health information systems' activity to protect against a cyber-attack, failure to implement an authentication process to safeguard its electronic protected health information, and failure to have security measures in place to protect electronic protected health information from unauthorized access when it was being transmitted electronically. Banner Health paid \$1,250,000 to OCR and agreed to implement a corrective action plan to address these potential violations of the HIPAA Security Rule and protect the privacy of patient information held by health care organizations, including Banner Health. "It is imperative that hospitals and other

Paid  
\$1,250,000  
for hacking.

“The potential violations specifically include:

- the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization,
- insufficient monitoring of its health information systems' activity to protect against a cyber-attack,
- failure to implement an authentication process to safeguard its electronic protected health information, and
- failure to have security measures in place to protect electronic protected health information from unauthorized access when it was being transmitted electronically.”

# Costs of Cybersecurity Lapse



The screenshot shows the TechTarget Health IT Security website. The header includes the TechTarget logo and 'HEALTH IT SECURITY | xtelligent HEALTHCARE MEDIA'. Navigation links include Home, News, Features, Interviews, and Pod. A secondary navigation bar lists IPAA and Compliance, Cybersecurity, Cloud, Mobile, Patient Privacy, Data Breaches, and Disaster Prepa. A prominent blue banner reads: 'Learn more about Data Encryption in our White Paper Library. Case studies, webcasts, eBooks and white papers all available now!' with a 'VIEW NOW' button. The TechTarget and Health IT Security logos are also present in the banner.

## Average Cost of Healthcare Data Breach Reaches \$11M

The cost of a healthcare data breach has soared 53% since 2020, IBM's latest report revealed.

Ponemon Institute

- Costs from:
  - Detection
  - Notification
  - Post-breach response
  - Lost business costs
- Highest cost across all industries.
- Ransomware cost average of \$5,130,000.
- Average of 277 days from detection to containment.

# HPH Cybersecurity Gateway

<https://hphcyber.hhs.gov/>

The screenshot shows the homepage of the HPH Cybersecurity Gateway. At the top left is the U.S. Department of Health and Human Services logo. The main heading reads "Welcome to Health & Human Services HPH Cybersecurity Gateway". Below this is a descriptive paragraph: "Connecting the Healthcare and Public Health (HPH) Sector with specialized healthcare specific cybersecurity information & resources from across the U.S. Department of Health and Human Services and other federal agencies." The background features a blue digital theme with various icons like a padlock, Wi-Fi, power, and a shopping cart. At the bottom, there are three callout boxes: "A NOTE FROM HHS", a list of "HPH Cybersecurity Performance Goals" with four checkmarks, and a megaphone icon with the text "Questions? Contact Us!".

 **Welcome to  
Health & Human Services**  
**HPH Cybersecurity Gateway**

*Connecting the Healthcare and Public Health (HPH) Sector with specialized healthcare specific cybersecurity information & resources from across the U.S. Department of Health and Human Services and other federal agencies.*

**A NOTE FROM HHS**

- ✓ **HPH**
- ✓ **Cybersecurity**
- ✓ **Performance**
- ✓ **Goals**

**Questions?  
Contact Us!**

# HHS Cybersecurity Performance Goals

<https://hphcyber.hhs.gov/documents/cybersecurity-performance-goals.pdf>

1/24/24



## HPH Cybersecurity Performance Goals

### Purpose

The Department of Health and Human Services (HHS) helps the Healthcare and Public Health (HPH) critical infrastructure sector adapt to the evolving threat landscape, and build a more resilient sector. As outlined in the HHS Healthcare Sector Cybersecurity Strategy, HHS is publishing these voluntary healthcare specific **Cybersecurity Performance Goals** (CPGs) to help healthcare organizations prioritize and implement cybersecurity practices.

These CPGs are a voluntary subset of cybersecurity practices that healthcare organizations, and healthcare delivery organizations can use to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were developed and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies (e.g., [Healthcare Industry Cybersecurity Practices](#), [Healthcare and Public Health Sector Cybersecurity Framework](#), [Healthcare Industry Cybersecurity Practices](#), and [the National Cybersecurity Strategy](#)). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals and health systems. For more information, see [Resiliency Landscape Analysis](#).

Voluntary

- Essential goals
- Enhanced goals

Download CPGs



Launch Tour



# NIST Cybersecurity Framework 2.0

<https://www.nist.gov/publications/nist-cybersecurity-framework-20-resource-overview-guide>

2/26/24

NIST

Search NIST

PUBLICATIONS

## NIST Cybersecurity Framework 2.0: Resource & Overview Guide

**Published:** February 26, 2024

**Author(s)**

Kristina Rigopoulos, Stephen Quinn, Cherilyn Pascoe, Jeffrey Marron, Amy Mahn, Daniel Topper

**Abstract**

The NIST Cybersecurity Framework (CSF) 2.0 can help organizations manage and reduce their cybersecurity risks as they start or update their cybersecurity program. This guide outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions that organizations can take. This guide is a supplement to the NIST CSF and is not intended to replace it.

**Citation:** Special Publication (NIST SP) - NIST SP 1299

**Report Number:** NIST SP 1299

**NIST Pub Series:** [Special Publication \(NIST SP\)](#)

**Pub Type:** NIST Pubs

[Download Paper](#)

### Includes

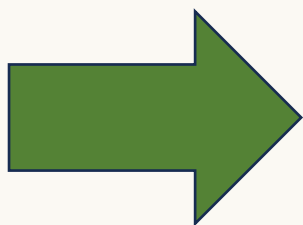
- Risk assessment guidelines
- Risk management guidelines
- HIPAA security rule considerations

# OCR Cybersecurity Guidance

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

The screenshot shows the U.S. Department of Health and Human Services website. The header includes the HHS logo and the tagline "Enhancing the health and well-being of all Americans". A search bar is located in the top right. Below the header is a navigation bar with links for "About HHS", "Programs & Services", "Grants & Contracts", and "Laws & Regulations". The main content area is titled "Health Information Privacy" and features four buttons: "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". Below this is a breadcrumb trail: "HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material > Cyber Security Guidance Material". A left sidebar menu is open, showing categories like "HIPAA for Professionals", "Regulatory Initiatives", "Privacy", "Security", "Summary of the Security Rule", "Security Guidance", and "Cyber Security Guidance". The main content area is titled "Cyber Security Guidance Material" and includes a sub-header "Cyber Security Guidance Material" and a paragraph: "In this section, you will find educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents." There are also social media icons for text, print, Facebook, and email.

- Cybersecurity Resources
- Cybersecurity Newsletters
  - Sanction policies (10/23)
  - Authentication (6/23)
  - Security rule incident procedures (10/22)
  - Defending against common cyber attacks (3/22)
  - Others
- Cyber incident response checklist



Sign up for OCR listserv at  
<https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html?language=es>

# OCR Cybersecurity Resources

- OCR webinar re How HIPAA Security Rule Can Help Defend Against Cyber-Attacks (10/30/23), <http://youtube.com/watch?v=VnbBxxyZLc8>
- OCR webinar re Risk Assessment (10/31/23), [https://kauffmaninc.zoom.us/webinar/register/WN\\_xaRWAC3qTYSyYAAbLL\\_ew](https://kauffmaninc.zoom.us/webinar/register/WN_xaRWAC3qTYSyYAAbLL_ew)
- CMS updated Security Risk Assessment Tool (version 3.4) (9/23), <https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool>
- OCR video re recognized security practices (10/31/22), <https://www.youtube.com/watch?v=e2wG7jUiRjE>



# HHS Cybersecurity Task Force

<https://www.hhs.gov/about/news/2023/04/17/hhs-cybersecurity-task-force-provides-new-resources-help-address-rising-threat-cyberattacks-health-public-health-sector.html>

## HHS Cybersecurity Task Force Provides New Resources to Help Address Rising Threat of Cyberattacks in Health and Public Health Sector

*Effort is led by the HHS 405(d) Program and the Health Sector Coordinating Council Cybersecurity Working Group (HSCC CWG), as a collaborative effort between the federal government and industry, to address cybersecurity in the health sector*

*Resources include a new platform, Knowledge on Demand, to provide free cybersecurity training to the health sector workforce as well as an updated Health Industry Cybersecurity Practices 2023 Edition and a Hospital Cyber Resiliency Initiative Landscape Analysis*

On April 17, 2023, The U.S. Department of Health and Human Services (HHS) 405(d) Program announced the release of the following resources to help address cybersecurity concerns in the Healthcare and Public Health (HPH) Sector:

- [Knowledge on Demand](#) – a new online educational platform that offers free cybersecurity trainings for health and public health organizations to improve cybersecurity awareness.
- [Health Industry Cybersecurity Practices \(HICP\) 2023 Edition](#) – a foundational publication that aims to raise awareness of cybersecurity risks, provide best practices, and help the HPH Sector set standards in mitigating the most pertinent cybersecurity threats to the sector.
- [Hospital Cyber Resiliency Initiative Landscape Analysis - PDF](#) – a report on domestic hospitals' current state of cybersecurity preparedness, including a review of participating hospitals benchmarked against standard

- Online educational platform for cybersecurity training
- Health Industry Cybersecurity Practices (2023)
  - Outlines top threats
  - Recommends best practices to prepare and fight against threats

# Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

<https://405d.hhs.gov/Documents/HICP-Main-508.pdf>

- Top threats
  - Social engineering
  - Ransomware
  - Loss or theft of equipment or data
  - Insider, accidental or malicious data loss
  - Attacks against network connected medical devices
- Best practices to protect against or respond to risks



# HHS Health Sector Cybersecurity Coordination Center (HC3),

<https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>

About HHS Programs & Services Grants & Contracts Laws & Regulations

[Home](#) > [About](#) > [Agencies](#) > [ASA](#) > [Office of the Chief Information Officer \(OCIO\)](#) > Health Sector Cybersecurity Coordination Center (HC3)

Assistant Secretary for Administration (ASA)

About ASA

EEO, Diversity & Inclusion +

Office of Business Management & Transformation (OBMT) +

Office of Human Resources (OHR) +

Office of the Chief Information Officer (OCIO) -

About OCIO

What We Do

Our Mission

Plans & Reports

Contact Us

Cybersecurity

Text Resize **A A A** Print Share

## Health Sector Cybersecurity Coordination Center (HC3)

### A Prescription for Health Sector Cybersecurity

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).



### HC3 Products

#### Threat Briefs

Highlights relevant cybersecurity topics and raise the HPH sector's situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics.

#### Sector Alerts

Provides high-level, situational background information and context for technical and executive audiences. Designed to assist the sector with defense of large scale and high level vulnerabilities.

- Threat briefs
- Sector alerts, e.g.,

- [\\*July 20, 2023 - Citrix ADC and Citrix Gateway Vulnerabilities Sector Alert - PDF](#)
- [\\*July 13, 2023 - AI, Cybersecurity and the Health Sector - PDF](#)
- [\\*July 13, 2023 - June 2023 Vulnerability Bulletin - PDF](#)
- [June 22, 2023 - SEO Poisoning Analyst Note - PDF](#)

- Additional resources

# Admin. for Strategic Preparedness & Response (ASPR)

<https://aspr.hhs.gov/cyber/Pages/default.aspx>

## Subscribe to ASPR's Cybersecurity Bulletins

Get information on cyber incidents, news, resources, engagement opportunities, and security updates sent right to your inbox.

 **Stay Informed. Subscribe Today.**

More alerts:  
Health Sector Coordination Center  
405(d) Mailing List

**Subscribe to  
bulletins**

**Learn to Improve Cybersecurity and Cyber Defense**

- Advisories concerning specific threats
- Links to cybersecurity resources

# OCR

## Implementing Sanction Policies

OCR emphasized use of sanction policies to help cybersecurity.

- Privacy and security rules require covered entities and business associates to have and apply appropriate sanctions against workforce members who fail to comply with HIPAA privacy and security requirements.
- Newsletter includes suggestions for drafting or revising sanction policies.
- May help avoid “willful neglect” penalties under HIPAA.

### October 2023 OCR Cybersecurity Newsletter

#### How Sanction Policies Can Support HIPAA Compliance

Last year, the Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) released a threat brief on the different types of social engineering<sup>1</sup> that hackers use to gain access to healthcare information systems and data.<sup>2</sup> The threat brief recommended several protective measures to combat social engineering, one of which was holding “every department accountable for security.” An organization's sanction policies can be an important tool for supporting accountability and improving cybersecurity and data protection. Sanction policies can be used to address the intentional actions of malicious insiders, such as the stealing of data by identity-theft rings, as well as workforce member failures to comply with policies and procedures, such as failing to secure data on a network server or investigate a potential security incident.

The HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) require covered entities and business

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2023/index.html>

# Information Blocking Rule



# 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
- **Effective 9/1/23, civil monetary penalties of up to \$1,000,000 per violation**

(42 CFR 1003.1420; see 88 FR 42820 (7/3/23);  
<https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/>)

## HEALTHCARE PROVIDERS

- “Appropriate disincentives” to be established by HHS.
- Proposed rule (88 FR 74947 (11/1/21))
  - **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 Penalties:

[https://www.healthit.gov/sites/default/files/2023-11/IB%20Disincentives%20for%20Providers%20Info%20Session20231115\\_508.pdf](https://www.healthit.gov/sites/default/files/2023-11/IB%20Disincentives%20for%20Providers%20Info%20Session20231115_508.pdf)

## **Proposed Rule 21<sup>st</sup> Century Cures Act: Establishment of Disincentives for Health Care Providers That Have Committed Information Blocking**

Office of the National Coordinator for Health Information Technology (ONC)

The Centers for Medicare & Medicaid (CMS)

# Info Blocking Rule: Examples

## **INFO BLOCKING**

- Refusing to timely respond to requests.
- Charging excessive fees.
- Imposing unreasonable administrative hurdles.
- Imposing unreasonable contract terms, e.g., EHR agreements, BAAs, etc.
- Implementing health IT in nonstandard ways that increase the burden.
- Others?

## **NOT INFO BLOCKING**

- Action required by law.
  - HIPAA, 42 CFR part 2, state privacy laws, etc.
  - Laws require conditions before disclosure and condition not satisfied, e.g., patient consent.
- Action is reasonable under the circumstances.
- Action fits within regulatory exception.

# Info Blocking Exceptions

[HTTPS://WWW.HEALTHIT.GOV/TOPIC/INFORMATION-BLOCKING](https://www.healthit.gov/topic/information-blocking)



**PREVENTING  
HARM  
EXCEPTION**



**PRIVACY  
EXCEPTION**



**SECURITY  
EXCEPTION**

**EXCEPTIONS THAT INVOLVE**  
not fulfilling requests to access,  
exchange, or use EHI



**INFEASIBILITY  
EXCEPTION**



**HEALTH IT  
PERFORMANCE  
EXCEPTION**

# 8

**EXCEPTIONS TO THE  
INFORMATION  
BLOCKING  
PROVISION**



**LICENSING  
EXCEPTION**



**FEES  
EXCEPTION**



**CONTENT AND  
MANNER  
EXCEPTION**

**EXCEPTIONS THAT INVOLVE**  
procedures for fulfilling requests  
to access, exchange, or use EHI

# Info Blocking Rule: OIG Enforcement Priorities

OIG will use the following priorities to select cases for investigation:

- resulted in, is causing, or had the potential to cause patient harm;
- significantly impacted a provider's ability to care for patients;
- was of long duration;
- caused financial loss to Federal health care programs, or other government or private entities; or
- was performed with actual knowledge.

(<https://oig.hhs.gov/reports-and-publications/featured-topics/information-blocking/>)

# Info Blocking Rule Guidance

<https://www.healthit.gov/topic/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)



# Artificial Intelligence 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
- “Garbage in, garbage out” → incorrect results
- Lack of transparency in algorithms, i.e., “black box” results
- **Data privacy**
- Others?

# Blueprint for AI Bill of Rights

<https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

10/22:

- Safe and effective systems.
- Algorithmic discrimination protections.
- **Data privacy**
- Notice and explanation
- Human alternatives, considerations and fallback





# Executive Order for Safe Use of AI

<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>



[Administration](#) [Priorities](#) [The Record](#)

OCTOBER 30, 2023

## Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

 BRIEFING ROOM  PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

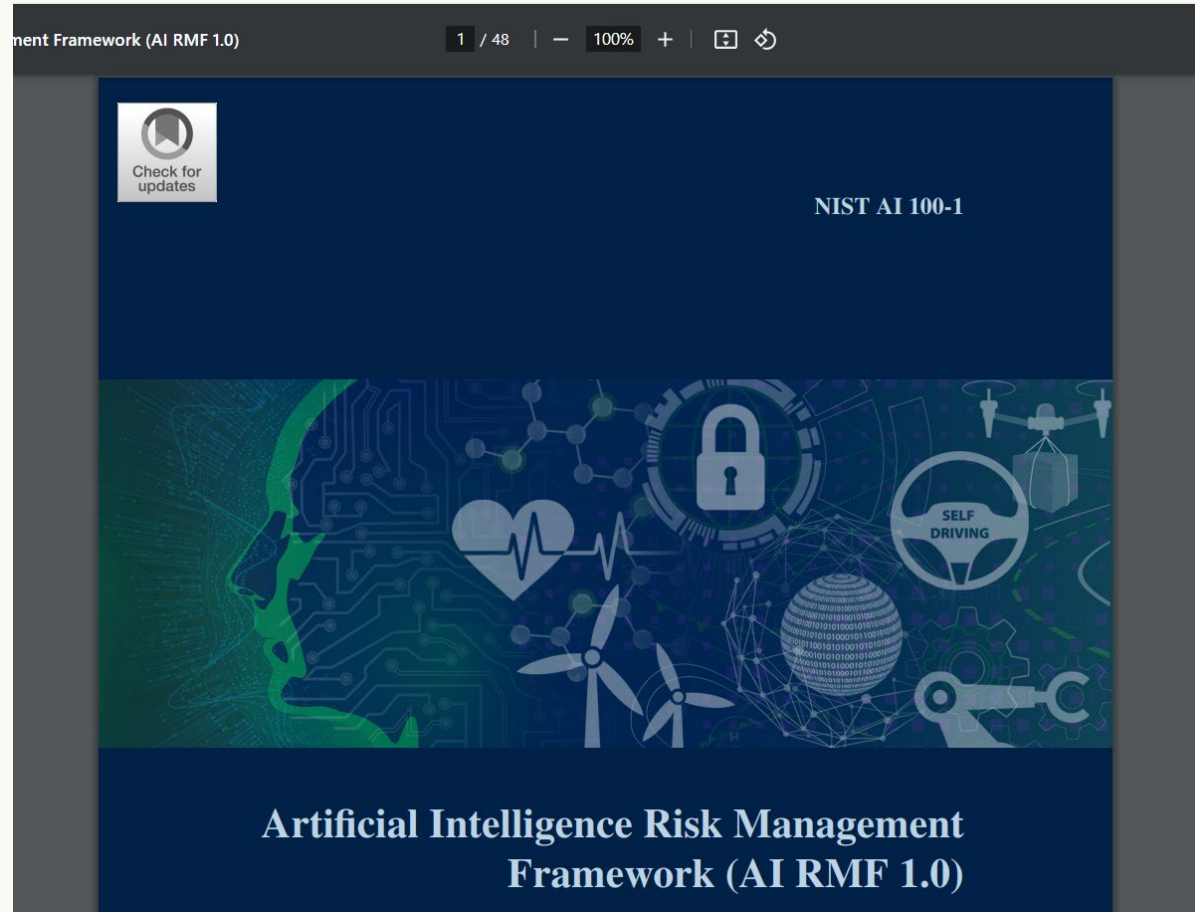
Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and

10/30/23

- Federal agencies to develop guidelines for developing safe, secure and trustworthy AI.
- Within 1 year, HHS to develop strategic plan including policies and potential regulations re deployment of AI in healthcare sector.

# NIST Artificial Intelligence Risk Management Framework

<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>



- Understanding and addressing risks, impacts and harms
- Challenges for AI risk management
- AI risks and trustworthiness
  - Valid and reliable
  - Safe
  - Secure and resilient
  - Accountable and transparent
  - Explainable and interpretable
  - **Privacy-enhanced**
  - Fair, with harmful bias managed

# Additional Resources



[HTTPS://WWW.HOLLAND  
HART.COM/HEALTHCARE](https://www.hollandhart.com/healthcare)

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other

The screenshot shows the Holland & Hart website's Healthcare section. At the top, the navigation bar includes the firm's logo, "People", "Capabilities", and a search bar with the text "Search by keyword". Below the navigation is a dark banner with the word "Healthcare" in large white letters. Underneath the banner are four menu items: "Overview", "Expertise", "People", and "News and Insights". The main content area is titled "Areas of Focus" and features three circular icons with corresponding text: a computer monitor icon for "WEBINAR RECORDINGS" (with a sub-link to health law recordings), an open book icon for "PUBLICATIONS" (with a sub-link to health law publications), and a caduceus icon for "IDAHO PATIENT ACT TIMELINE". To the right of this section are two rectangular buttons: "Mergers and Acquisitions" and "Real Estate". Further down, there is a section for "Primary Contacts" which includes a portrait of Kim Stanger and a list of legal services such as HIPAA, mergers, and government investigations. The footer of the page features the Holland & Hart logo.

# Questions?



Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

[kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com)