

COMPLIANCE UPDATE 2024-2025



Kim C. Stanger

(12.24)

Today's Presenter



Kim C. Stanger

Partner, Holland & Hart LLP

(208) 383-3913

kcstanger@hollandhart.com

Kim Stanger is a partner in the Boise office of Holland & Hart LLP and the chair of the firm's Health Law Group. Mr. Stanger helps clients navigate complex state and federal regulations and practical uses facing the healthcare industry, including transactional, compliance, and administrative matters.

He is consistently named as one of the Best Lawyers in America® for Health Care Law by U.S. News and a Mountain States Super Lawyer. He is a member of the American Health Law, Past President of the Idaho Bar Association Health Law Section, and a frequent author and speaker on health law-related issues.

Disclaimer

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

- OIG Compliance Guidance
- Fraud and Abuse Issues
- HIPAA and Data Privacy
 - Reproductive Health Rule
 - Online Tracking Guidance
 - Substance Use Disorder Rule
- Data Security
- Info Blocking Rule Penalties
- TCPA
- Artificial Intelligence (AI)



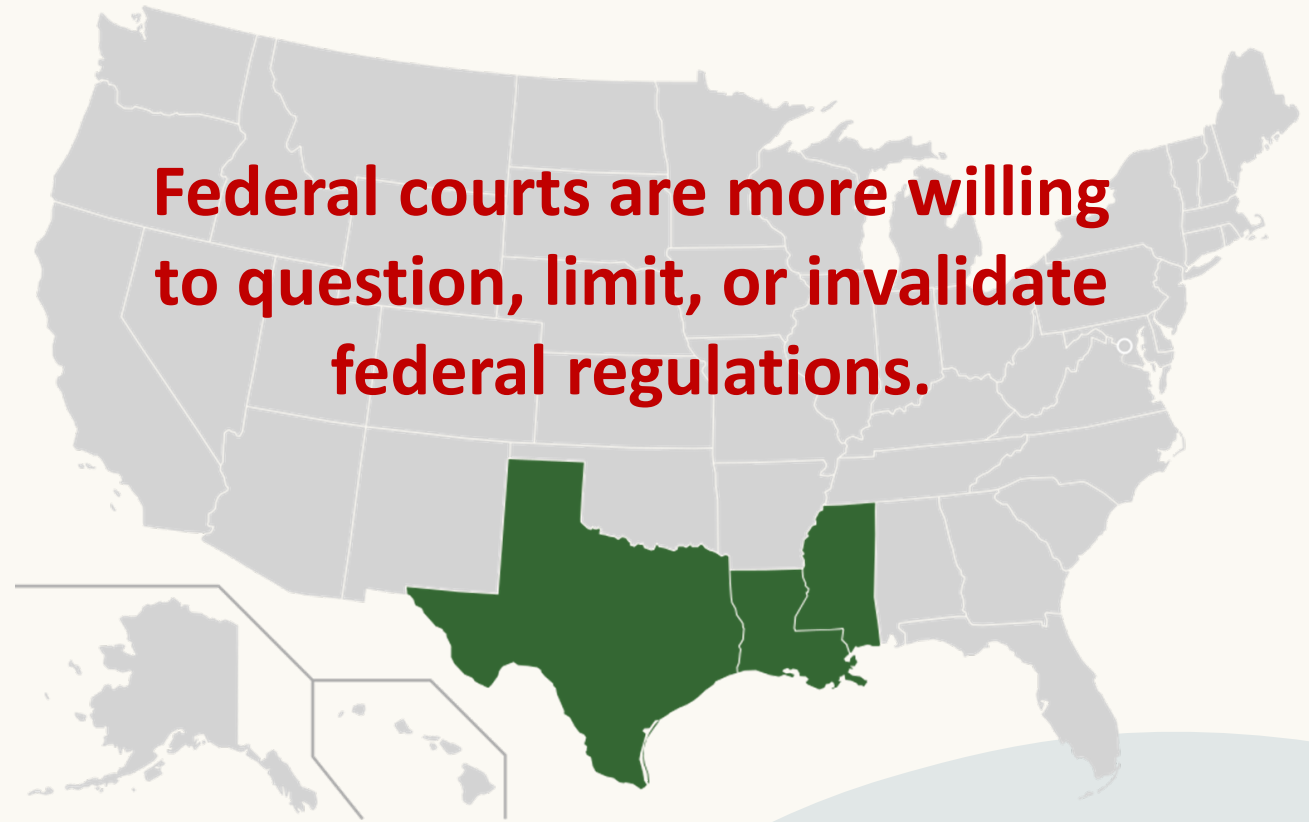
- Telehealth
- Anti-Discrimination Rules
 - 1557
 - Rehab Act
 - Conscience Rules
- OSHA and Workplace Violence
- Noncompetes



CAUTION:
The Rules may change....



**Trump administration may
change or undermine existing
rules.**



OIG General Compliance Program Guidance



U.S. Department of Health and Human Services
Office of Inspector General



[Submit a Complaint](#)

[About OIG](#) ▾

[Reports](#) ▾

[Fraud](#) ▾

[Compliance](#) ▾

[Exclusions](#) ▾

[Newsroom](#) ▾

[Careers](#) ▾

[COVID-19 Portal](#)

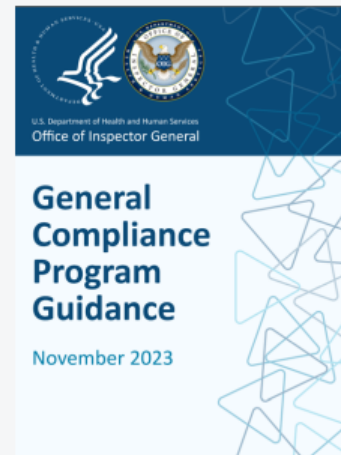
General Compliance Program Guidance

The General Compliance Program Guidance (GCPG) is a reference guide for the health

Watch for industry-specific guidance.

You may download the guidance in whole, or access individual sections below.

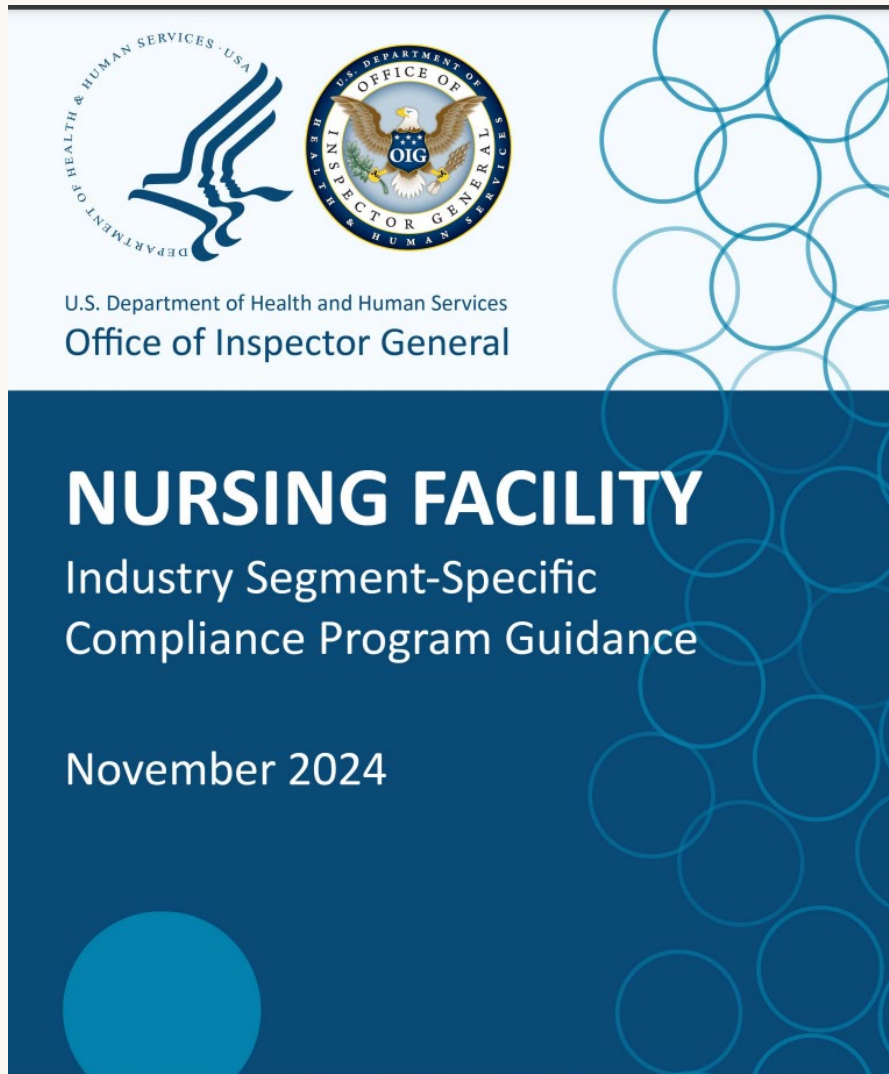
[Download Complete Guidance](#)



Individual Sections

1. Overview of Federal Laws
2. Elements of Successful Compliance Program
3. Adaptions for Small and Large Entities
4. Other Compliance Considerations
5. OIG Resources and Processes

OIG Compliance Program Guidance: Nursing Facilities



- In 11/24, OIG issued the Compliance Program Guidance for Nursing Facilities.
- Available at <https://oig.hhs.gov/documents/compliance/10038/nursing-facility-icpg.pdf>.

DOJ Corporate Compliance Program Guidance

- Updated 9/24/24.
- DOJ Evaluation of Corporate Compliance Program
 - Risk assessment
 - Policies and procedures
 - Training and communication
 - Confidential reporting and investigation process
 - Third party management
 - Commitment by management
 - Improvement, testing and review
 - Analysis and remediation
 - Others

(<https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl>)

**U.S. Department of Justice
Criminal Division**
Evaluation of Corporate Compliance Programs
(Updated September 2024)

Introduction

The “Principles of Federal Prosecution of Business Organizations” in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include “the adequacy and effectiveness of the corporation’s compliance program at the time of the offense, as well as at the time of a charging decision” and the corporation’s remedial efforts “to implement an adequate and effective corporate compliance program or to improve an existing one.” JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation’s compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (*e.g.*, monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a

Fraud and Abuse



False Claims Act



United States
Attorney's Office
Southern District of Indiana

About ▾ News ▾ Divisions Programs ▾

Justice.gov > U.S. Attorneys > Southern District of Indiana
Million to Settle Alleged False Claims Act Violations

PRESS RELEASE

Community Health Network Agrees to Pay \$345 Million to Settle Alleged False Claims Act Violations

“the United States alleged that the compensation Community paid to its cardiologists, cardiothoracic surgeons, vascular surgeons, neurosurgeons, and breast surgeons was well above fair market value, that Community awarded bonuses to physicians that were tied to the number of their referrals, and that Community submitted claims to Medicare for services that resulted from these unlawful referrals.”

False Claims Act (FCA)

- Cannot knowingly submit a false claim for payment to the federal govt, e.g.,
 - Not provided as claimed
 - Substandard care
 - Failure to comply with applicable regulations
- Must report and repay an overpayment within the later of 60 days or date cost report is due.

(31 USC 3729; 42 USC 1320a-7a(a); 42 CFR 1003.200)

Penalties

- Repayment plus interest
- **Civil penalty of \$13,946* to \$27,894* per claim**
- **Admin penalty \$24,947* per claim failed to return**
- 3x damages
- Exclusion from Medicare/Medicaid
(42 USC 3729; 42 USC 1320a-7a(a); 42 CFR 1003.210; 45 CFR 102.3; 89 FR 9766)
- Potential *qui tam* lawsuits
 - ✓ ***But see U.S. ex rel. Zafirov v. Florida Med. Associates LLC* (M. Dist. Fla. 9/30/24), holding *qui tam* lawsuits as unconstitutional.**

CMS Report and Repay Rule

REPORT AND REPAY RULE

- A person who has received an overpayment must report and return the overpayment by the later of:
 - The date which is 60 days after the date on which the overpayment was identified; or
 - The date any corresponding cost report is due, if applicable.

(42 CFR 401.305)

NEW RULES

- Person has identified an overpayment if:
 - Has actual knowledge of info; or
 - Acts in deliberate ignorance or in reckless disregard of truth of info.

(42 CFR 401.305(a)(2))

 - Replaces “reasonable diligence” standard
- 60-day reporting period suspended for up to 180 days during timely, good faith investigation. (42 CFR 401.305(b))
 - Replaces prior guidance that 60 days does not begin to run until after identify and quantify overpayment.

HIPAA and Patient Privacy



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

(45 CFR 102.3, 160.404; 85 FR 2879)

Recent HIPAA Resolutions

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

Top HIPAA Risks

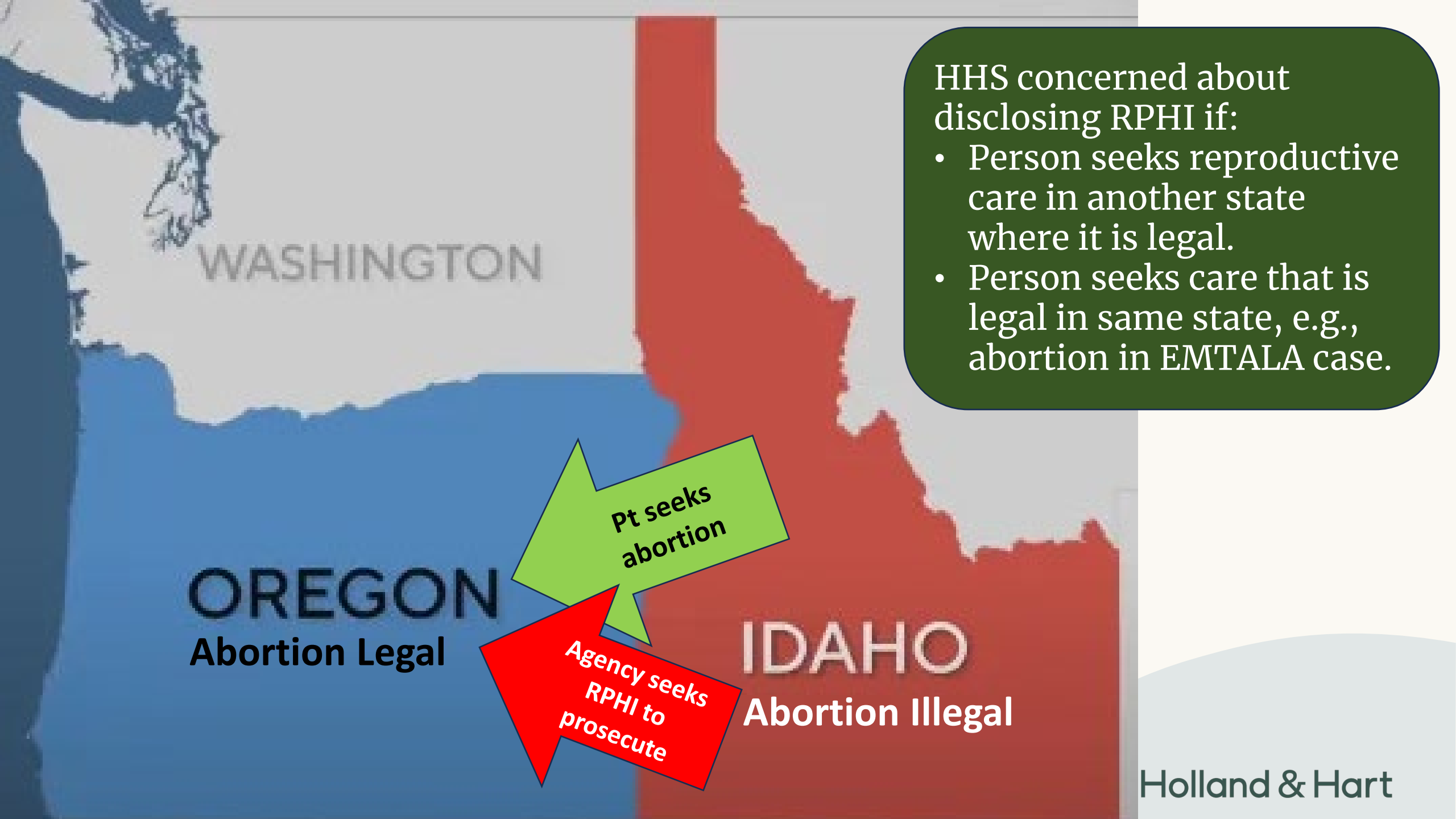


1. Cyberattacks
2. Security rule violations
3. Right of access violations

Date	Conduct	
10/31/24	Ambulance services hit with ransomware attack.	
10/31/24	Plastic surgeons hit with ransomware attack.	\$500,000
10/17/24	Dentist office failed to provide timely access to records.	\$70,000
10/3/24	Hospital hit with ransomware attack.	\$240,000
9/26/24	Eye and Skin Center hit with ransomware attack	\$250,000
8/1/24	EMS provider failed to provide timely access to records.	\$115,200
7/1/24	Health system hit with ransomware attack.	\$950,000
4/1/24	Essex Residential Care failed to provide personal rep 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

HIPAA Reproductive Health Rule





WASHINGTON

OREGON
Abortion Legal

IDAHO
Abortion Illegal

Pt seeks abortion

Agency seeks RPHI to prosecute

HHS concerned about disclosing RPHI if:

- Person seeks reproductive care in another state where it is legal.
- Person seeks care that is legal in same state, e.g., abortion in EMTALA case.

HIPAA Reproductive Health Rule

- Must comply by **12/23/24** unless rule is stayed or stricken by court.
- Applies to PHI re “reproductive health care”, i.e., “healthcare that that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes.”

(45 CFR 160.103)

- **If reproductive healthcare was legal, covered entities and business associates may not use or disclose reproductive health care PHI (“RPHI”) for purposes of criminal, civil or administrative liability or investigation for mere act of seeking, obtaining or providing reproductive health care.**

(45 CFR 164.502(a)(5))

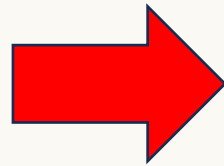
- **Must obtain attestation from persons seeking RPHI for purposes of criminal, civil or administrative investigation or liability to confirm purpose and legality.**

(45 CFR 164.509)

Reproductive Health Rule: Required Attestation

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

(45 CFR 164.509)



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

Reproductive Health Rule: Required Attestation

Valid attestation =

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

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

Reproductive Health Rule: OCR Model Attestation



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

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

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

Prohibited Purposes. Covered entities and their business associates may not use or disclose PHI for the following purposes:

- (1) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- (2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care.
- (3) To identify any person for any purpose described in (1) or (2).⁹

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

Model Instructions

Information for the Person Requesting the PHI

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

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

In the meantime, HHS apparently intends to enforce the Rule.

Home

Podcasts

Media Guidelines for HHS Employees

FOR IMMEDIATE RELEASE
November 26, 2024

Contact: HHS Press Office

202-690-6343

media@hhs.gov

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

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

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

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

OCR is sending a message:

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

Lawsuits Filed in Texas Federal Court

Texas v. HHS (ND Tex. 9/4/24)

- Argues that HIPAA statute doesn't limit how covered entities may share PHI with state govt investigators.

Purl v. HHS (ND Texas 10/21/24)

- Argues no statutory authority for the rule and it is arbitrary and capricious under the APA.

We will likely receive a preliminary decision before the 12/23/24 compliance date. Stay tuned...

OCR Education

- Final Rule
- Press Release
- Fact Sheet
- Webinar + Slides
- Model Attestation
- Social Media Resources



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office for Civil Rights

December 5, 2024

Compliance With Most Provisions of the HIPAA Privacy Rule to Support Reproductive Health Care Privacy is Required by December 23, 2024

On April 22, 2024, the U.S. Department of Health and Human Services, Office for Civil Rights announced a final rule, entitled the *HIPAA Privacy Rule to Support Reproductive Health Care Privacy*. The rule strengthens privacy protections for medical records and health information for individuals who are seeking, obtaining, providing, or facilitating lawful reproductive health care.

Health Plans, health care clearinghouses, and most health care providers and business associates are required to be in compliance with most provisions of the final rule by December 23, 2024. In order to ensure the public and regulated entities understand their rights and responsibilities, OCR has posted several documents and videos on its [website](#) and [YouTube channel](#) including:

- [Final Rule](#)
- [Press Release](#)
- [Fact Sheet \(en español\)](#)
- [Director's message on YouTube \(en español\)](#)
- [Webinar](#)
- Social Media Toolkit: [HIPAA Privacy Rule to Support Reproductive Health Care Privacy - PDF | en español - PDF](#)
- [June 20, 2024, Presentation on Final Rule \(Slides\) - PDF](#)
- [Director's message on Attestation Compliance](#)
- For HIPAA Covered Entities or Business Associates: [Model Attestation for a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care - PDF](#)

HIPAA and Administrative Requests



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 Online Tracking Technologies



Online Tracking Concerns



The HIPAA Journal is the
most authoritative and indepe

[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.

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.

See our data here.

GitHub

HIPAA and Online Tracking

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



About HHS Programs & Services Grants & Contracts Laws & Regulation

Health Information Privacy

HIPAA for Individuals

Filing a Complaint

HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > U

HIPAA for Professionals	
Regulatory Initiatives	
Privacy	+
Security	+
Breach Notification	+
Compliance & Enforcement	+
Special Topics	+
Patient Safety	+

Use of 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

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

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

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

HIPAA and Online Tracking

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

The screenshot shows the U.S. Department of Health and Human Services (HHS) website. At the top left is the HHS logo and the text "U.S. Department of Health and Human Services" with the tagline "Enhancing the health and well-being of all Americans". A navigation bar contains links for "About HHS", "Programs & Services", "Grants & Contracts", and "Laws & Regulation". Below this is the "Health Information Privacy" section, which includes two buttons: "HIPAA for Individuals" and "Filing a Complaint". A breadcrumb trail reads: "HHS > HIPAA Home > For Professionals > Privacy > Guidance Materials > U". A table of contents is visible on the left side of the page.

HIPAA for Professionals	
Regulatory Initiatives	
Privacy	+
Security	+
Breach Notification	+
Compliance & Enforcement	+

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

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>)

Online Tracking Lawsuits

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

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

Marianne Kolbasuk McGee (HealthInfoSec) • January 16, 2024

Share Tweet Share Credit Eligible Get Permission

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

NPR Illinois Fresh Air

Small western Illinois hospitals face federal lawsuits over online tracking

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

Share

Possible Theories

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

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**



Substance Use Disorder Records

New rule:

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

(89 FR 12472)

Applies to:

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

Aligns 42 CFR part 2 with HIPAA.

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

(42 CFR part 2)

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.

42 CFR part 2 Resources

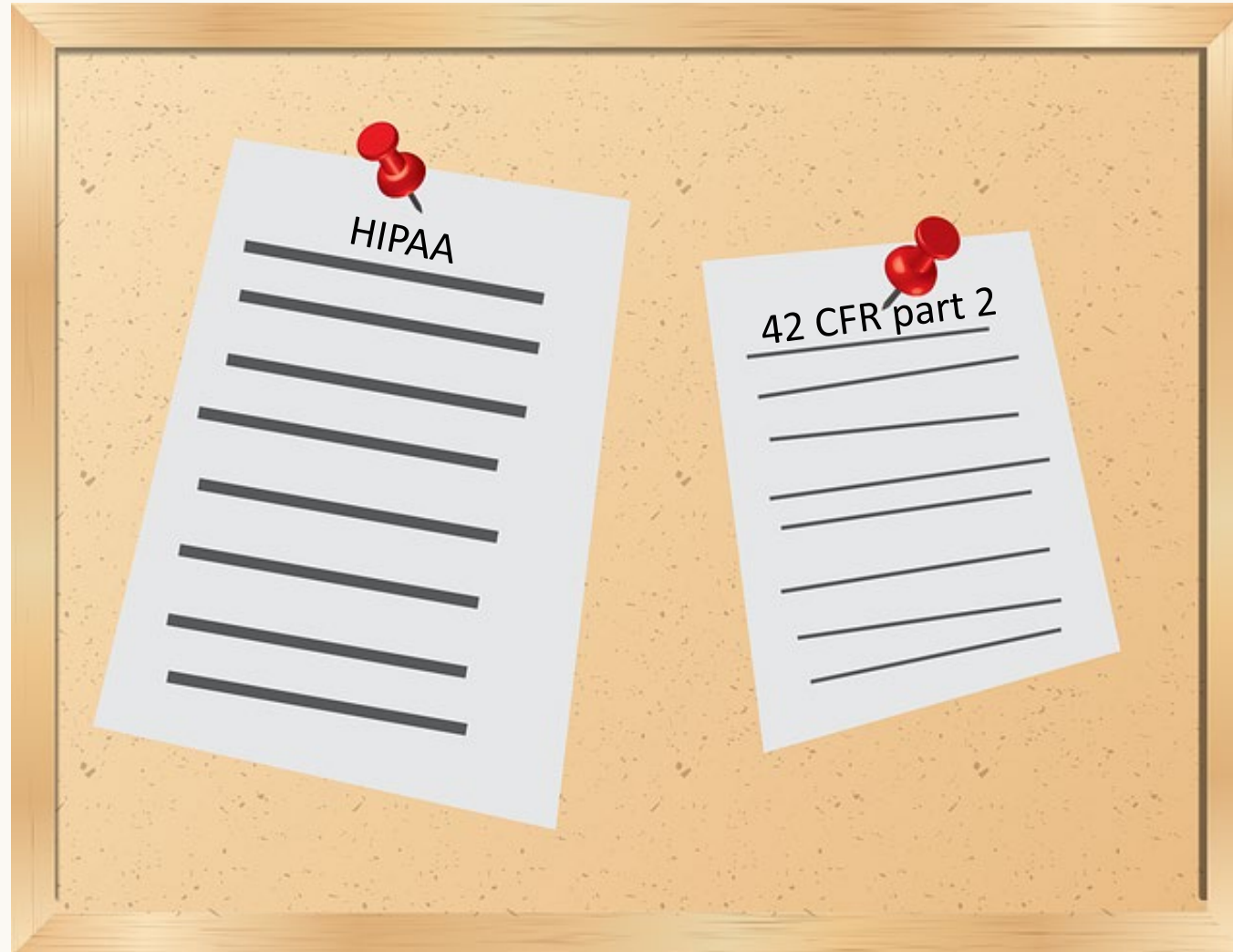
HTTPS://WWW.SAMHSA.GOV/ABOUT-US/WHO-WE-ARE/LAWS-REGULATIONS/CONFIDENTIALITY-REGULATIONS-FAQS

The screenshot shows the SAMHSA website. At the top, there is a navigation bar with links for Home, Site Map, and Contact Us. Below this is a search bar and a menu with categories like Find Help, Practitioner Training, Public Messages, Grants, Data, Programs, Newsroom, About Us, and Publications. The main content area is titled "Substance Use Confidentiality Regulations" and includes a link to a fact sheet: "The Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? (PDF | 1.6 MB)". Below this is a section titled "Applying the Substance Use Confidentiality Regulations" with a link to a document: "Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE) (PDF | 381 KB)".

HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SPECIAL-TOPICS/HIPAA-PART-2/INDEX.HTML

The screenshot shows the HHS website. At the top, there is a navigation bar with links for About HHS, Programs & Services, Grants & Contracts, and Laws & Regulations. Below this is a search bar and a menu with categories like Health Information Privacy, HIPAA for Individuals, Filing a Complaint, HIPAA for Professionals, and Newsroom. The main content area is titled "HIPAA and Part 2" and includes a link to a document: "Notice of Proposed Rulemaking to revise the Confidentiality of Substance Use Disorder Patient Records regulations. The".

HIPAA and SUD Rules: Notice of Privacy Practices



HIPAA and SUD Rules: Notice of Privacy Practices

- Reproductive Health Rule: modified NPP requirements to accommodate SUD Rule changes.
- SUD Rule: 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.
- Other covered entities must update their NPP.
(45 CFR 164.520(a)(2))
 - Must comply by **2/16/26**.
 - ✓ *Check applicable regulations when drafting updated NPP.*
 - ✓ *Watch for new NPP requirements when final HIPAA revisions are published.*
 - ✓ *OCR plans to publish model NPP.*

HIPAA Priorities

- On 10/23/24, HHS and NIST hosted conference, “Safeguarding Health Information: Building Assurance Through HIPAA Security”.
- OCR identified priorities, including:
 - Conduct and document appropriate risk analyses
 - Obtain and maintain appropriate business associate agreements (BAAs)
 - Provide patients and personal reps with timely access
 - Implement appropriate access controls and info system activity review to protect against and/or identify potential breaches
- Watch for new security rule requirements shortly.

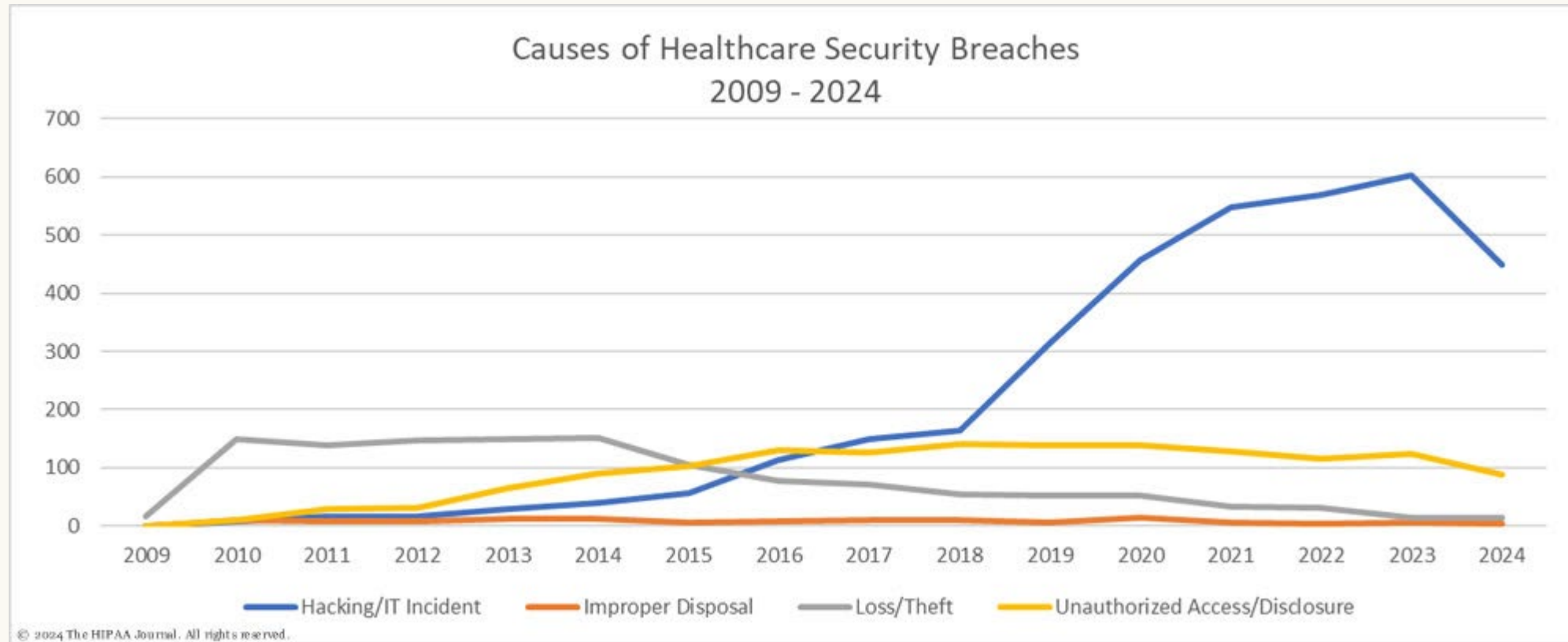
Data Security



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/>

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 Health IT Security logo is also present in the bottom right of 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.

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 Ram

Change Healthcare cyberattack fallout continues

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



☰ CNN politics SCOTUS Congress Facts First 2024 Elections

Cyberattack forces Idaho hospital to send ambulances elsewhere



Change Cyberbreach

<https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html>

Change Healthcare Cybersecurity Incident Frequently Asked Questions

Updated as of October 24, 2024

1. Why did OCR issue the Dear Colleague letter about the Change Healthcare cybersecurity incident?

A: Given the unprecedented magnitude of this cyberattack, its widespread impact on patients and health care providers nationwide, and in the interest of patients and health care providers, OCR issued the [Dear Colleague](#) addressing the following:

- OCR confirmed that it prioritized and opened investigations of Change Healthcare and UnitedHealth Group focused on whether a breach of protected health information (PHI) occurred and on the entities' compliance with the [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\) Rules](#). OCR did this because of the cyberattack's unprecedented impact on patient care and privacy.
- OCR's investigation interests in other entities that partnered with Change Healthcare and UHG is secondary. It would include those [covered entities](#) that have [business associate](#) relationships with Change Healthcare and UHG, and those organizations that are business associates to Change Healthcare and UHG.

FAQs address items such as:

- Covered entities' obligation to report the breach.
- Delegating breach reporting to its business associate (e.g., Change).
- Resolving breach notification with Change.

HHS Strategy Paper

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



Coming Soon?

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.

Recent HIPAA Resolutions

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

Date	Conduct	Resolution
12/10/24	Health care clearinghouse data available through Google search.	\$250,000
10/31/24	Ambulance services hit with ransomware attack.	\$90,000
10/31/24	Plastic surgeons hit with ransomware attack.	\$500,000
10/17/24	Dentist office failed to provide timely access to records.	\$70,000
10/3/24	Hospital hit with ransomware attack.	\$240,000
9/26/24	Eye and Skin Center hit with ransomware attack	\$250,000
8/1/24	EMS provider failed to provide timely access to records.	\$115,200
7/1/24	Health system hit with ransomware attack.	\$950,000
4/1/24	Essex Residential Care failed to provide personal rep 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 and mailed ID cards to wrong patients.	\$1,300,000
8/24/23	UnitedHealthcare failed to timely provide copy of records.	\$80,000

HPH Cybersecurity Gateway

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



**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 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](#), and [the National Cybersecurity Strategy](#)). The HPH CPGs directly address common attack vectors against U.S. domestic hospitals as identified in the [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>

NIST

Search NIST

PUBLICATIONS

2/26/24

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 to implement it. This guide outlines specific outcomes that organizations can achieve to address risk. Other NIST resources help explain specific actions to 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

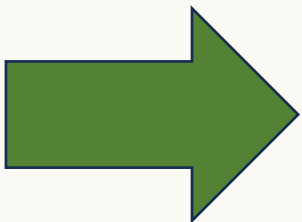
- Risk assessment guidelines
- Risk management guidelines
- HIPAA security rule considerations

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 a search bar. A navigation bar contains links for About HHS, Programs & Services, Grants & Contracts, and Laws & Regulations. Below this is a section for Health Information Privacy with buttons for HIPAA for Individuals, Filing a Complaint, HIPAA for Professionals, and Newsroom. The main content area shows a breadcrumb trail: HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material > Cyber Security Guidance Material. A left sidebar menu lists: HIPAA for Professionals, Regulatory Initiatives, Privacy (+), Security (-), Summary of the Security Rule, Security Guidance, and Cyber Security Guidance. The main heading is 'Cyber Security Guidance Material' with a sub-heading: '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.' Social media icons for text, print, Facebook, and email are visible.



- 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

<https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html>

- [OCR HIPAA Security Rule Guidance Material](#) – This webpage provides educational materials to learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information. Materials include a Recognized Security Practices Video, Security Rule Education Paper Series, HIPAA Security Rule Guidance, OCR Cybersecurity Newsletters, and more.
- [OCR Video on How the HIPAA Security Rule Protects Against Cyberattacks](#)  – This video discusses how the HIPAA Security Rule can help covered entities and business associates defend against cyberattacks. Topics include breach trends, common attack vectors, and findings from OCR investigations.
- [OCR Webinar on HIPAA Security Rule Risk Analysis Requirement](#)  – This webinar discusses the HIPAA Security Rule requirements for conducting an accurate and thorough assessment of potential risks and vulnerabilities to electronic protect health information and reviews common risk analysis deficiencies OCR has identified in its investigations.
- [HHS Security Risk Assessment Tool](#) – This tool is designed to assist small- to medium-sized entities in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule.
- [Factsheet: Ransomware and HIPAA](#) – This resource provides information on what is ransomware, what covered entities and business associates should do if their information systems are infected, and HIPAA breach reporting requirements.
- [Healthcare and Public Health \(HPH\) Cybersecurity Performance Goals](#) – These voluntary, health care specific cybersecurity performance goals can help health care organizations strengthen cyber preparedness, improve cyber resiliency, and protect patient health information and safety.

OCR Cybersecurity Newsletter (10/24)

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2024/index.html>

Cautions against:

- Social engineering, e.g.,
 - Phishing
 - Smishing (texts)
 - Baiting
 - Deepfakes (AI cloning)
- Guidance for minimizing exposure
- HIPAA security rule compliance

October 2024 OCR Cybersecurity Newsletter

Social Engineering: Searching for Your Weakest Link

Cyber threats targeting individuals often take the form of social engineering, where attackers attempt to convince someone to engage in actions or reveal information that can put themselves and their organizations at risk. Social engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks or taking an action (e.g., clicking a link, opening a document).¹ Between 2019 and 2023 large breaches (i.e., breaches of unsecured protected health information (PHI) involving 500 or more individuals) reported to the HHS Office for Civil Rights (OCR) as a result of hacking or IT incidents increased 89%.² Cybersecurity is often framed solely as a technology issue where protection can be provided by simply purchasing the newest security tool. But according to a recent report, 68% of breaches involved attacks on humans, not technology.³

Social engineering attackers attempt to manipulate their targets by using an ever-evolving arsenal of technology and deceit. Such attacks can take many forms including emails, texts, calls, or even videos that appear to be from trusted individuals, companies, or institutions. Using such manipulative techniques can often bring an attacker quicker and easier success than attempting to breach an organization's cyber defenses. In short, social engineering is so prevalent because it works. The end game for social engineering attackers is varied. Attackers could be seeking money, to disrupt an organization's operations, or to gain access to sensitive information. This newsletter discusses common social engineering threats and how individuals and HIPAA regulated entities can defend against them.

Phishing is one of the most frequent social engineering attacks. A phishing attack attempts to trick individuals into providing sensitive information electronically. This is most often accomplished through the use of email where the attacker sends an email purporting to be from a trustworthy source, for example, an organization's HR department, a

Proposed Legislation: HISAA

NATIONAL LAW REVIEW

ABOUT THE NLR QUICK LINKS NLR NEWSLETTERS TRENDING LAW NEWS CAREER CENTER

Health Infrastructure Security and Accountability Act

**HISAA: New Federal Law Introduced That
Would Create Significant New
Cybersecurity Requirements for HIPAA
Covered Entities and Business Associates**

by: Allen R. Killworth of Epstein Becker & Green, P.C. - *Health Law Advisor*

CURRENT PU

Post Your Public

PUBLIC NOTICE
BUSINESS SALE

HISAA would provide:

- Mandatory minimum cybersecurity standards for healthcare providers.
- Annual independent cybersecurity audits.
- HHS security audits.
- Top executives certify compliance annually.
- Eliminate statutory caps on HHS fines.
- Funded by user fees.

FTC and Data Security





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 Enforcement of Privacy and Security

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

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

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

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

FTC Health Breach Notification Rule (HBNR)

- Requires vendors of personal health info to provide notice of breach to consumers and FTC.
 - Generally, does not apply to entities covered by HIPAA (covered entities and business associates)
- Modified rule effective **7/29/24**
 - Confirms HBNR applies to health apps, online services, and other technologies not covered by HIPAA.
 - “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.

(16 CFR part 316; 89 FR 47028)

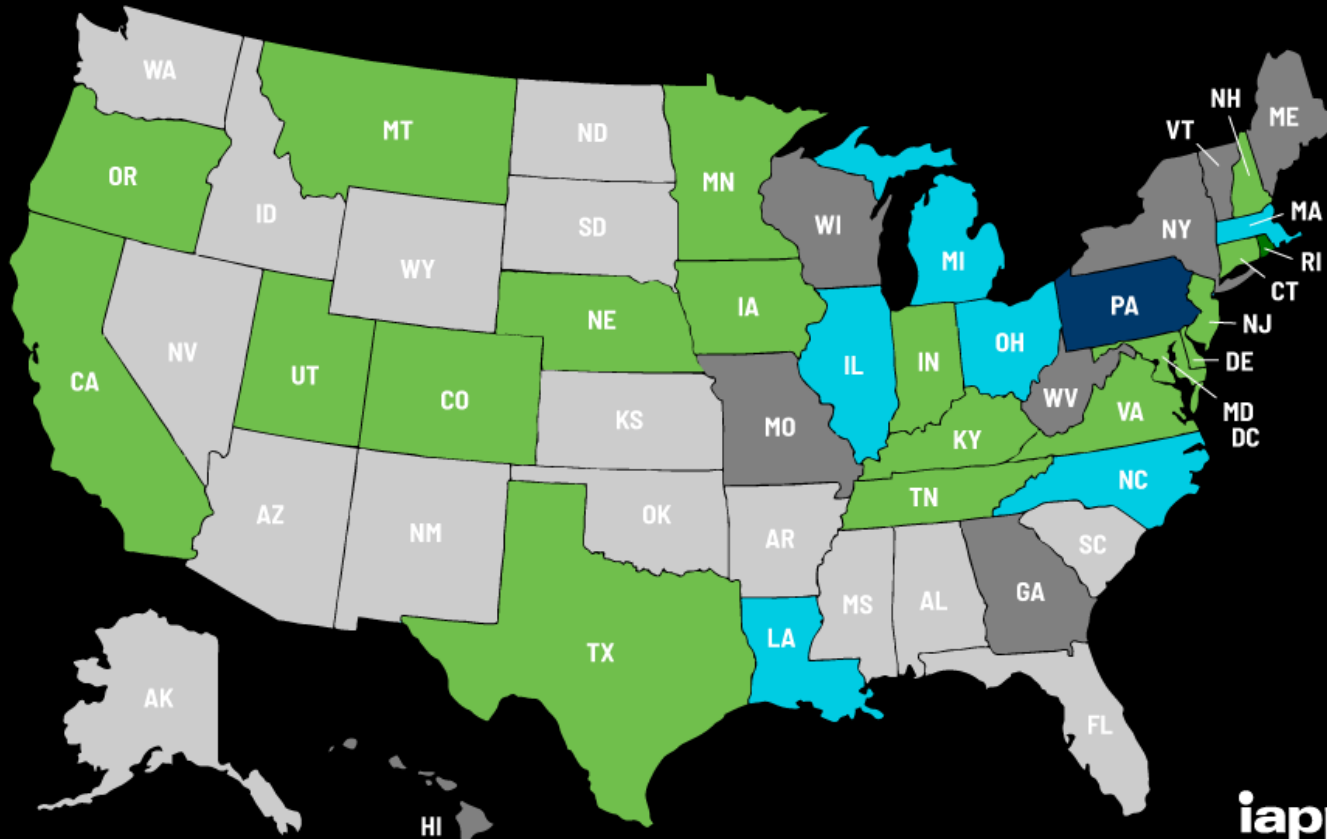
- **GoodRx pays \$1,500,000 for failing to report unauthorized disclosure of consumer health data to Facebook, Google, and others.**
- **Easy Healthcare (Premom ovulation tracking app) shared info with third parties, including AppsFlyer and Google.**

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/>

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
- Civil monetary penalties of up to \$1,000,000 per violation

(42 CFR 1003.1420)

HEALTHCARE PROVIDERS

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

Info Blocking Rule Guidance

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

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

Hospital Price Transparency Rules



Hospital Price Transparency Rules



U.S. Department of Health and Human Services

Office of Inspector General



[Submit a Complaint](#)

[About OIG](#) ▾ [Reports](#) ▾ [Fraud](#) ▾ [Compliance](#) ▾ [Exclusions](#) ▾ [Newsroom](#) ▾ [Careers](#) ▾

[Home](#) > [Reports and Publications](#) > [All Reports and Publications](#) > [2024](#) > Not All Selected Hospitals Complied With the Hospital Pr...

Not All Selected Hospitals Complied With the Hospital Price Transparency Rule

Issued on 11/05/2024 | Posted on 11/08/2024 | Report number: A-07-22-06108

Report Materials

 [Full Report \(PDF, 2.2 MB\)](#)

 [Report Highlights \(PDF, 333.0 KB\)](#)

OIG Report:

- 34/100 hospitals are noncompliant.
- Recommends CMS implement enforcement mechanisms.

Hospital Price Transparency

- Hospital must publish list of the hospital's "standard charges".
 - See regulations for specifics.
- Must be posted through hospital's website.
- Must update at least annually.
(45 CFR 180.70)

Penalties

- Written warning, corrective action plan, fines
- Increased penalties
 - Small hospitals (≤ 30 beds)
 - Maximum of \$300 per day
 - Large hospitals (> 30 beds)
 - Minimum of \$10 per bed per day, and
 - Maximum of \$5,500 per day.
 - Range of \$109,500 to \$2,007,500 per year

(45 CFR 180.70-.90; CMS Fact Sheet, <https://www.cms.gov/newsroom/press-releases/cms-oppasc-final-rule-increases-price-transparency-patient-safety-and-access-quality-care>)

Price Transparency: Enforcement

Hospital price
transparency

Enforcement actions

- 15 reported actions at <https://www.cms.gov/priorities/ke y-initiatives/hospital-price-transparency/enforcement-actions>
- Penalties range from \$56,940 to \$979,000.
- In most cases, appears CMS sent warning letter first.

Enforcement Actions

Below is a list of civil monetary penalty (CMP) notices issued by CMS.

Date Action Taken	Hospital Name	CMP Amount	Effective Date
2022-06-07	Northside Hospital Atlanta	\$883,180.00	2021-09-02
2022-06-07	Northside Hospital Cherokee	\$214,320.00	2021-09-09
2023-04-19	Frisbie Memorial Hospital	\$102,660.00	2022-10-24
2023-04-19	Kell West Regional Hospital <i>Under Review *</i>	\$117,260.00	2022-07-08
2023-07-20	Falls Community Hospital &Clinic	\$70,560.00	2023-01-06
2023-07-20	Fulton County Hospital <i>Under Review *</i>	\$63,900.00	2022-12-22
2023-07-24	Community First Medical Center <i>Under Review *</i>	\$847,740.00	2022-06-22
2023-08-22	Hospital General Castaner <i>Under Review *</i>	\$101,400.00	2022-09-19
2023-08-22	Samaritan Hospital - Albany Memorial Campus <i>Under Review *</i>	\$56,940.00	2023-06-06

Price Transparency Resources

<https://www.cms.gov/hospital-price-transparency/hospitals>

- Regulations
- FAQs
- Technical guidance
- Updated sample formats
- Quick reference checklist
- Sample corrective action plan response

The screenshot shows the CMS.gov website interface. At the top right, there are navigation links: Home | About CMS | Newsroom | Archive | Help | Print. Below this is the CMS.gov logo and the text "Centers for Medicare & Medicaid Services". A search bar with the text "Search CMS" and a "Search" button is located to the right of the logo. Below the search bar is a row of eight yellow navigation buttons: Medicare, Medicaid/CHIP, Medicare-Medicaid Coordination, Private Insurance, Innovation Center, Regulations & Guidance, Research, Statistics, Data & Systems, and Outreach & Education. Below these buttons is a breadcrumb trail: Home > Hospital Price Transparency. A dark blue navigation bar contains links for Home, Hospitals, Consumers, Resources, and Contact Us. The main content area features a large blue circle with a white dollar sign and a price tag icon, followed by the heading "Hospital Price Transparency". Below the heading is a dark blue box with white text that reads: "Hospital price transparency helps Americans know the cost of a hospital item or service before receiving it. **Starting January 1, 2021**, each hospital operating in the United States will be required to provide clear, accessible pricing information online about the items and services they provide in two ways:" followed by a numbered list: "1. As a comprehensive machine-readable file with all items and services." and "2. In a display of shoppable services in a consumer-friendly format." At the bottom of the page, there is a line of text: "This information will make it easier for consumers to shop and compare prices across hospitals and estimate the cost of care before going to the".

Telephone Consumer Protection Act (TCPA)



Telephone Consumer Protection Act (TCPA)

Generally prohibits:

- Using automatic phone dialing system (“robo-call”) to call a hospital emergency line or guest room, cell phone, or other line if recipient is charged for call.
- Robo-calling or using pre-recorded voice to deliver message unless:
 - Emergency,
 - Have prior written consent,
 - Have consent if made by tax-exempt nonprofit organization, or
 - “health care” message by HIPAA-covered entity or business associate.

(47 USC 227; 47 CFR 64.1200)

Penalties

- Recipient of more than 1 call within prior 12-month period may sue for:
 - Actual damages or \$500 per call, whichever is greater.
- State AGs may sue.

(47 USC 227)

TCPA: Healthcare Message Exception

- Exception only applies to three types of calls by a healthcare provider or its business associates without a patient's prior authorization:
 - calls to describe a health-related product or service that is provided by the covered entity making the communication;
 - calls for treatment of the individual (e.g., appointment reminder; prescription refill reminders; etc.); and
 - calls for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
- **For healthcare calls, must limit to no more than 1 call per day up to 3 calls per week.**
(47 CFR 64.1200; <https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#healthcare>)

Telephone Consumer Protection Act (TCPA)

Effective **4/11/25**:

- Consumers may revoke consent to robocalls and robotexts “in any reasonable manner” — including use of the words: stop, quit, end, revoke, opt out, cancel, or unsubscribe.
- Callers must honor do-not-call and revocation requests “as soon as practicable” — no later than 10 business days after the request.
- Text-senders may send one text message in response to a revocation request confirming or clarifying the scope of the request within five minutes.

(47 CFR 64.1200; <https://public-inspection.federalregister.gov/2024-23605.pdf>; 89 FR 15756)

TCPA Resources

<https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule>



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

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

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

Complying with the Telemarketing Sales Rule

Tags: [Advertising and Marketing](#) | [Telemarketing](#)

Related Rules: [Telemarketing Sales Rule](#)

[Introduction](#)

[Who Must Comply with the Amended TSR?](#)

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

Artificial Intelligence in Healthcare



Watch for
developments

FEDERAL INITIATIVES

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

STATE INITIATIVES

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

Telehealth



Telehealth



- Many of the **Medicare** COVID-19 waivers are currently due to **expire 12/31/24**
 - Covered telehealth services.
 - Originating site requirements.
 - Eligible distant site telehealth providers.
 - Coverage of audio-only services.
 - In-person visit requirements.
 - Others?

Check your telehealth services to ensure that you comply.

(See <https://www.cms.gov/medicare/coverage/telehealth> and <https://www.cms.gov/files/document/mln901705-telehealth-services.pdf>)

- CMS allows physicians to provide direct supervision remotely until 12/31/25.
- DEA allows providers to prescribe controlled substances without in-person visit until 12/31/25.
- **States and private payers may have other requirements.**

Telehealth

As a general rule, telehealth provider must comply with both

- Law of state in which **telehealth provider is located**,

and

- Law of state in which **patient is located**.
 - States want to protect patients.
 - Likely sufficient contacts to establish jurisdiction over telehealth provider



Beware

- Licensure
- Permissible telehealth methods
- Provider-patient relationship
- Scope of practice
- Standard of care
- Informed consent
- Remote prescribing
- Credentialing telehealth providers
- Reimbursement and payment parity
- Malpractice liability and insurance
- Corporate practice of medicine
- Others?

Center for Connected Health Policy,
<https://www.cchpca.org/>



Look up policy by:

Topic ▾

Federal

State ▾



Summary of federal and state laws

Understanding telehealth policy

Get to know how the laws, regulations, and Medicaid programs work in your state.



How we work



Resources & reports



Ask a policy expert



All telehealth policies



COVID-19 actions



Pending legislation

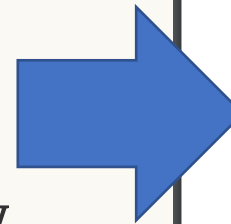
Telehealth policy finder

Know what you're searching for? Find the policies and regulations that impact you.

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.

EMTALA



EMTALA

- CMS published new optional signage available at <https://www.cms.gov/medicare/regulations-guidance/legislation/emergency-medical-treatment-labor-act>.
- Signage must:
 - Specify the rights of individuals with EMCs who come to the ED.
 - Indicate whether the facility participates in the Medicaid program;
 - Clear and in simple terms and language(s) that are understandable by the population served by the hospital; and
 - Posted in a place or places likely to be noticed by all individuals entering the ED or waiting for exam and treatment (e.g., entrance, admitting area, waiting room, treatment area).

(QSO-24-17-EMTALA)



KNOW YOUR RIGHTS
EMERGENCY MEDICAL TREATMENT AND LABOR ACT (EMTALA)

 **EMTALA GUARANTEES ACCESS TO EMERGENCY MEDICAL SERVICES FOR INDIVIDUALS WHO PRESENT TO A HOSPITAL EMERGENCY DEPARTMENT REGARDLESS OF AN INDIVIDUAL'S ABILITY TO PAY**
It also provides for appropriate transfers if the presenting facility is unable to provide the care or services necessary to stabilize a medical condition.

 **ALL INDIVIDUALS MUST BE SCREENED**
All individuals who present to a hospital emergency department must be screened by Qualified Medical Personnel to determine the presence or absence of an emergency medical condition. EMTALA applies until either (1) the medical screening exam does not identify an emergency medical condition or (2) the patient is provided with stabilizing treatment and/or an appropriate transfer.

 **STABILIZING TREATMENT MUST BE PROVIDED**
Hospitals must make sure the patient is provided with stabilizing treatment (within the capabilities of the hospital's staff and facilities) before they can initiate a transfer to another hospital or medical facility or before they can discharge the patient.

 **NO DELAY IN EXAMINATION AND TREATMENT**
Hospitals may not delay providing an appropriate medical screening examination or stabilizing medical treatment for any reason, including to ask about an individual's method of payment or health insurance status.

 **FOUR REQUIREMENTS FOR APPROPRIATE TRANSFER**
A patient with an emergency medical condition may only be transferred when these four requirements are met:

- The transferring hospital provides the medical treatment, within its capacity, to minimize the medical risks (and in the case of a woman in labor, the medical risks of the fetus as well).
- The receiving medical facility has available space and qualified personnel for the treatment and agrees to accept the transfer.
- The transferring hospital sends all medical records related to the emergency condition that are available at the time of the transfer and any other records not yet available as soon as practicable.
- The patient is transferred using appropriate personnel and transportation, including the use of necessary and medically appropriate life support measures during the transfer.

Anyone can file an EMTALA complaint with the [State Survey Agency](#). The State Survey Agency will investigate the issue and, when appropriate, verify corrective action is taken to ensure the hospital is in compliance with EMTALA. Visit the [Quality, Safety and Education Portal \(QSEP\)](#) to view an [EMTALA overview video](#) at [qsep.cms.gov](#)

Non-Discrimination Rules



Anti-Discrimination Laws

LAWS

- Civil Rights Act Title VI
- Americans with Disability Act
- Age Discrimination Act
- **Affordable Care Act § 1557**
 - **HHS issued new rules on 5/6/24.**
 - **Effective 7/5/24**
(45 CFR part 92; 89 FR 37522)
- **Rehabilitation Act § 504**
 - **HHS issued new rules on 5/9/24.**
 - **Effective 7/8/24**
(45 CFR part 84; 89 FR 40066)
- State discrimination laws

Apply if receive federal
money, e.g., participate in
Medicare/Medicaid

RISKS

- Persons with disabilities
- Persons with limited English proficiency
- Sex discrimination
- Physical access to facilities and equipment
- Websites and mobile apps
- Service animals
 - Dogs and mini-horses
 - Not emotional support animals

Anti-Discrimination Laws

DISABILITIES

- Must provide reasonable accommodation to ensure effective communication and accessibility.
 - **Accessibility**
 - **Auxiliary aids**
 - **Modifications to policies or processes**
- Includes person with patient.
- May not charge patient.
- May not rely on person accompanying patient.

LIMITED ENGLISH

- Must provide meaningful access
 - **Interpreter**
 - **Translate key documents**
- Includes person with patient.
- May not charge patient.
- May not require patient to bring own interpreter.
- May not rely on person accompanying patient.

New 1557 Rule

- Recipients of federal financial assistance (HHS money) may not discriminate on the basis of race, color, national origin, sex*, age and disability.

(45 CFR part 92)

- Specific requirements re:
 - Coordinator and grievance procedure
 - Policies and procedures
 - Training employees
 - **Notice of nondiscrimination**
 - **Notice of availability of language assistance**
 - Persons with limited English proficiency
 - Persons with disabilities
 - **Equal access on the basis of sex***
 - **Facility accessibility**
 - **Info and communication technology accessibility**
 - **Patient care decision support tools**

New 1557 Rule: Legal Challenges

- In *Tennessee v. Becerra*, No. 1:24cv161-LG-BWR (S.D. Miss.), the court stayed nationwide the specific 1557 regulations to the extent they “extend discrimination on the basis of sex to include discrimination on the basis of gender identity” ... and enjoined HHS from enforcing the 2024 Final Rule “to the extent that the final rule provides that ‘sex’ discrimination encompasses gender identity.”
- In *Texas v. Becerra*, No. 6:24-cv-211-JDK (E.D. Tex.), the court stayed nationwide the 1557 regulations that would otherwise obligate providers to follow those rules related to gender identity and sexual orientation.

<https://www.hhs.gov/civil-rights/for-providers/resources-covered-entities/index.html>

- *And remember that first Trump administration eviscerated prior 1557 Rules...*



New 1557 Rule

By 7/5/24

- Provide meaningful access, e.g., interpreters and translators; auxiliary aids, facility accessibility, information technology, telehealth.
- Provide equal access on basis of sex (subject to litigation).

By 11/2/24

- If have 15+ employees, designate 1557 Coordinator.
- Publish Notice of Nondiscrimination on website, in physical location, and upon request.

By 5/1/25

- Don't discriminate in decision support tools (e.g., AI).
- Train employees re 1557 policies and procedures and document training.

By 7/5/25

- Implement written 1557 policies and procedures.
- Publish Notice of Availability of Services in English + at least 15 most common languages.

(45 CFR part 92)

1557 Rule Resources

<https://www.hhs.gov/civil-rights/for-providers/resources-covered-entities/index.html>

Civil Rights

Information for Individuals

Filing a Complaint

Information for Providers

[HHS](#) > [Civil Rights Home](#) > [For Providers](#) > Resources for Covered Entities

Civil Rights for Providers of Health Care and Human Services

Provider Obligations

Civil Rights Clearance for Medicare Provider Applicants

Compliance & Enforcement

Training

Resources for Covered Entities

Pursuant to decisions by various district courts regarding the 2024 Final Rule implementing Section 1557, entitled Nondiscrimination in Health

Programs and Activities, 89 Fed. Reg. 27,522 (May 6, 2024) ("2024 Final Rule"), provisions are stayed or enjoined as indicated below.

- Sample policies and procedures
 - *Effective communication*
 - *Grievance*
 - *Language access*
 - *Nondiscrimination policy*
 - *Reasonable modification*
- Sample notices
 - *Availability of language assistance and auxiliary aids*
 - *Notice of nondiscrimination*

New Rehab Act Rule

- Recipients of federal financial assistance (HHS money) may not discriminate on the basis of disability.
- “Disability” construed very broadly.

(45 CFR part 92)

- Specific requirements re:
 - Notice and signage requirements.
 - Communication (e.g., auxiliary aids, interpreters)
 - Facility accessibility
 - Service animals
 - **Medical treatment (e.g., devaluing worth of disabled persons)**
 - **Mobility devices**
 - **Medical diagnostic equipment**
 - **Kiosks**
 - **Web and mobile apps**

New Rehab Act Rule

By 7/8/24

- Cannot discriminate based on disability, i.e., must provide meaningful access to persons with disability, e.g., facility accessibility, interpreters, auxiliary aids, service animals, etc.
- Newly purchased or leased medical diagnostic equipment (MDE) must meet accessibility standards.
- At least 10% but no less than one (1) MDE must meet Standards for Accessible MDE.

By 5/11/26

- If have 15+ employees, must ensure web content and mobile apps comply with Web Content Accessibility Guidelines (WCAG) unless fundamental alteration or undue burden.

By 7/8/26

- At least one exam table and weight scale must meet Standards for Accessible MDE.

By 5/10/27.

- All recipients must ensure web content and mobile apps comply with WCAG.

(45 CFR part 92)

New Rehab Act Rule

<https://www.hhs.gov/civil-rights/for-individuals/disability/section-504-rehabilitation-act-of-1973/index.html>

Section 504 of the Rehabilitation Act of 1973

The Office for Civil Rights (OCR) enforces Section 504 of the Rehabilitation Act of 1973 (Section 504), which prohibits discrimination on the basis of disability in the provision of benefits and services as amended 29 USC § 794, against otherwise qualified disabled individuals. This includes in programs and activities receiving financial assistance from HHS 45 CFR 84; and programs or activities conducted by HHS 45 CFR 85.

OCR Finalizes Section 504 Rule to Stop Against Disability Discrimination

- Fact Sheets
- Press Release

ADA Rules for State and Local Govts

<https://www.ada.gov/resources/2024-08-08-mde-fact-sheet/>



Fact Sheet: New Rule on the Accessibility of Medical Diagnostic Equipment Used by State and Local Governments

August 08, 2024

On August 9, 2024, the Federal Register published the Department of Justice's (Department) [final rule](#) updating the regulation for Title II of the Americans with Disabilities Act (ADA). The [final rule](#) has specific requirements about

Table of contents

Fact Sheet: New Rule on the Accessibility of Medical Diagnostic Equipment Used by State and Local Governments

Reasons for the Rule

Highlights of this Rule's Requirements

How Long State and Local Government Entities Have to Comply with the Rule

ADA Information and Resources

Print this page



Anti-Discrimination Laws: Enforcement

- Same enforcement procedures as apply to Title VI of the Civil Rights Act of 1964
 - HHS (OCR) conducts complaint investigations and compliance reviews.
 - Agency may force corrective action through settlement agreements.
 - Possible loss of federal funding.
 - Possible civil or administrative penalties by DOJ.
 - Private lawsuits for injunctive relief and/or damages.

HHS Office for Civil Rights Issues Notice of Violation to Puerto Rico Psychiatric Hospital for Failure to Comply with Federal Civil Rights Laws on Disability

OCR takes enforcement action against San Juan Capestrano Hospital to strengthen access to health services and ensure effective communication for individuals who are deaf or hard of hearing

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced the issuance of a Letter of Finding and Notice of Violation against the San Juan Capestrano Hospital, following a thorough investigation, for violating disability civil rights laws when it failed to provide a patient with a sign language interpreter, under the Americans with Disabilities Act (Section 1557).

“Effective communication for every patient.”

On 9/12/24, HHS asserted claims against a hospital for failing to provide a sign language interpreter; handwritten notes, lip reading, or gestures were insufficient.

Anti-Discrimination Laws: Recent OCR Enforcement

Date	Alleged Conduct	Resolution
12/11/24	University of California failed to accommodate children with disabilities.	Policies and Training
10/10/24	Maryland failed to accommodate persons with disability in programs	Policy and training
9/12/24	Psych hospital failed to provide sign language interpreter.	Policy and training
8/5/24	Imaging network denied mammography patient who used wheelchair.	Policy and training
6/21/24	Puerto Rico agency failed to provide sign language interpreters.	Policy and training
6/4/24	ENT practice failed to provide aids to persons with hearing challenges.	Policy and training
11/13/23	SNF allegedly denied admission to individuals because they were taking Suboxone or methodone to treat opioid use disorder.	Policy and training
8/30/23	Home Health agency denied home health care services based on HIV status	Policy and training
8/8/23	Pa DHS denied application as foster parent because she receives SUD medication	Policy and training
6/16/23	CVS and Walgreens failed to fill prescriptions for methotrexate and misoprostol unrelated to abortion	Policy and training
3/23/23	Dearborn OBGYN refused request for sign language interpreter, cancelled appointment and terminated her as patient	Policies, training \$7,500 in damages

New Conscience Rules

- Various federal laws prohibit:
 - Coercion or discrimination on basis of conscience, i.e., based on religious or moral convictions.
 - Requiring individual providers to participate in actions they find religiously or morally objectionable (e.g., abortions or assisted suicide).
- Apply to healthcare providers, patients and participants in federal programs.
- Effective **3/11/24**:
 - Persons may file a complaint with OCR for investigation.
 - Violations may result in loss of federal funding.
 - “Best practice” to post notice of federal conscience protections at location, in personnel handbooks and training, applications, etc.
 - OCR provides sample notice. (45 CFR part 88 App. A)

(45 CFR part 88; 89 FR 2078)

New Conscience Rule

<https://www.hhs.gov/conscience/conscience-protections/index.html>



U.S. Department of
Health and Human Services

Enhancing the health and well-being of all Americans

Search

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

Conscience and Religious Freedom

[Conscience Protections](#)

[Religious Freedom](#)

[Filing a Complaint](#)

[Newsroom](#)

[HHS](#) > [Conscience and Religious Freedom Home](#) > [Conscience Protections](#)

Conscience and Religious
Freedom



- Summary of Conscience Laws
- Rule and Commentary
- Press Release
- Fact Sheet
- OCR webinar

Employment Issues



Employee v. Contractor

Some potential ramifications

- Federal and state wage claims.
- IRS tax liability
- Workers compensation
- Liability for person's misconduct
- Stark, Anti-Kickback and EKRA compliance
 - Rules differ for employee v. contractor
- HIPAA obligations
- Other?

Ensure personnel are properly classified as employees v. contractors

- State common law standards
- DOL standards
- IRS standards
- HIPAA “common law of agency”
- Other?

Employee v. Independent Contractor

DEPT OF LABOR

- Effective **3/11/24**, new rules for evaluating employees v. contractors for purposes of FLSA. (29 CFR part 795; 89 FR 1638)

The screenshot shows the U.S. Department of Labor website. The header includes the U.S. Department of Labor logo and navigation links for 'ABOUT US', 'CONTACT US', and 'ESPAÑOL'. Below the header is a search bar labeled 'Search WHD'. A blue navigation bar contains links for 'TOPICS', 'WORKER RIGHTS', 'FOR EMPLOYERS', 'RESOURCES', 'INTERPRETIVE GUIDANCE', 'STATE LAWS', and 'NEWS RELEASES'. The main content area features a breadcrumb trail: 'WHD > Wages and the Fair Labor Standards Act > Misclassification of Employees as Independent Contractors Under the Fair Labor Standards Act > Final Rule: Employee or Independent Contractor Classification Under the Fair Labor Standards Act, RIN 1235-AA43'. The title of the page is 'Final Rule: Employee or Independent Contractor Classification Under the Fair Labor Standards Act, RIN 1235-AA43'. The introductory text states: 'On January 10, 2024, the U.S. Department of Labor published a final rule, effective March 11, 2024, revising the Department's guidance on how to analyze who is an employee or independent contractor under the Fair Labor Standards Act (FLSA). This final rule rescinds the Independent Contractor Status Under the Fair Labor Standards Act'.

IRS

- Existing rules for evaluating employees v. contractors for purposes of taxes.

(<https://www.irs.gov/businesses/small-businesses-self-employed/independent-contractor-self-employed-or-employee>)

The screenshot shows the IRS website. The header includes the IRS logo and navigation links for 'Help', 'News', 'English', 'Charities & Nonprofits', and 'Tax Pros'. Below the header is a search bar. A blue navigation bar contains links for 'File', 'Pay', 'Refunds', 'Credits & Deductions', and 'Forms & Instructions'. The main content area features a breadcrumb trail: 'Home / File / Businesses and self-employed / Small business and self-employed / Independent contractor (self-employed) or employee?'. The title of the page is 'Independent contractor (self-employed) or employee?'. Below the title are language options: 'English | Español | 中文(简体) | 中文(繁體) | 한국어 | Русский | Tiếng Việt | Kreyòl Ayisyen'. The page is divided into sections: 'Individuals' (It is critical that business owners correctly determine whether the individuals providing services are employees or independent contractors.) and 'Businesses and self-employed' (Generally, you must withhold and deposit income taxes, social security taxes, and...). A 'Related' section is also visible with the link 'Businesses with employees'.

Noncompetition Clauses

- FTC rule: effective **9/4/24**
 - It is unfair method of competition to enter or enforce a post-termination non-compete against workers or senior executives.
 - Subject to limitations.
 - Employer must provide notice to workers otherwise covered by non-compete that it will not be enforced.

(16 CFR 910)

- On 7/23/24, federal court in Pennsylvania upheld the FTC rule. (*ATS Tree Services, LLC v. FTC*, No. 24-1743 (E.D. Pa. 2024))
- **On 8/20/24, federal court in Texas struck down the rule and enjoined the FTC from enforcing it.** (*Ryan LLC v. FTC*, CV 3:24-CV-00986E (N.D. Tex. 2024))

✓ *Stay tuned....*

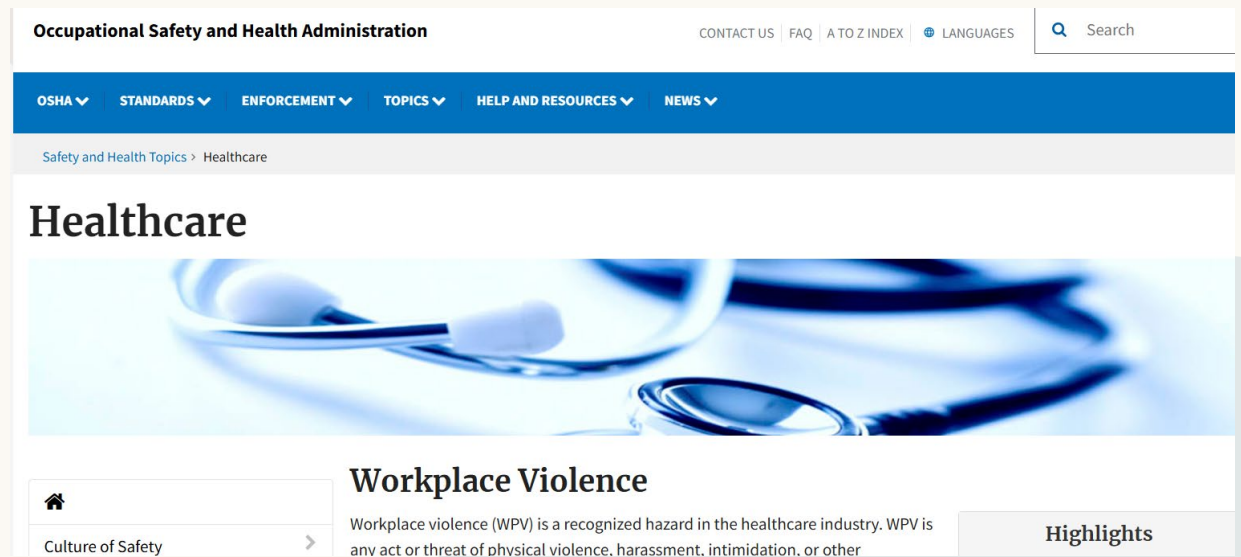
Workplace Violence

OSHA is expected to propose new standards for employers to address workplace violence in healthcare settings.

In the meantime:

- OSHA general duty standard applies.
- See guidance at

<https://www.osha.gov/healthcare/workplace-violence>.



The screenshot shows the Occupational Safety and Health Administration (OSHA) website. The header includes the OSHA logo, navigation links for CONTACT US, FAQ, A TO Z INDEX, LANGUAGES, and a search bar. A blue navigation bar contains dropdown menus for OSHA, STANDARDS, ENFORCEMENT, TOPICS, HELP AND RESOURCES, and NEWS. Below this, a breadcrumb trail reads 'Safety and Health Topics > Healthcare'. The main heading is 'Healthcare', followed by a blue-tinted image of a stethoscope and pills. A section titled 'Workplace Violence' features a home icon and a 'Culture of Safety' link. The text states: 'Workplace violence (WPV) is a recognized hazard in the healthcare industry. WPV is any act or threat of physical violence, harassment, intimidation, or other'. A 'Highlights' button is visible in the bottom right corner.

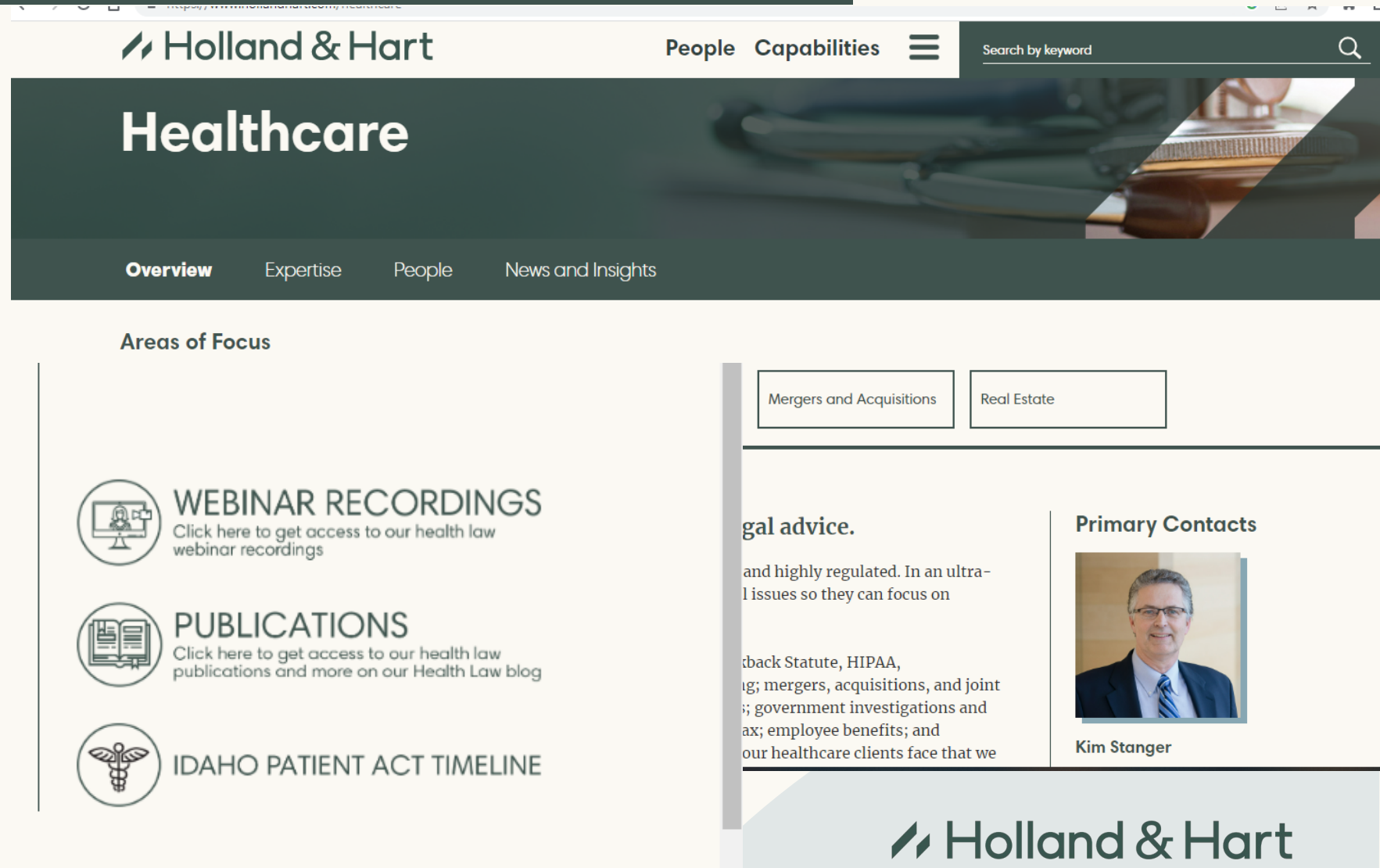
Additional Resources



HTTPS://WWW.HOLLAND HART.COM/HEALTHCARE

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other



The screenshot shows the Holland & Hart website's Healthcare section. The header includes the firm's logo, navigation links for 'People' and 'Capabilities', and a search bar. The main heading is 'Healthcare', with sub-navigation for 'Overview', 'Expertise', 'People', and 'News and Insights'. The 'Areas of Focus' section features three icons: a computer monitor for 'WEBINAR RECORDINGS', an open book for 'PUBLICATIONS', and a caduceus for 'IDAHO PATIENT ACT TIMELINE'. A sidebar on the right contains buttons for 'Mergers and Acquisitions' and 'Real Estate', a 'Legal advice' section with text about highly regulated issues, and a 'Primary Contacts' section featuring a photo of Kim Stanger.

Holland & Hart

People Capabilities


Search by keyword


Healthcare


Overview Expertise People News and Insights

Areas of Focus

Mergers and Acquisitions Real Estate

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


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

 **IDAHO PATIENT ACT TIMELINE**

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

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

Primary Contacts



Kim Stanger

Holland & Hart

Questions?



Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com