

Compliance Update: 2023 Year in Review

December 2023

| Presented by Kim C. Stanger



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 has been repeatedly awarded the Best Lawyers® Health Care Law "Lawyer of the Year" for Boise. 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.



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.

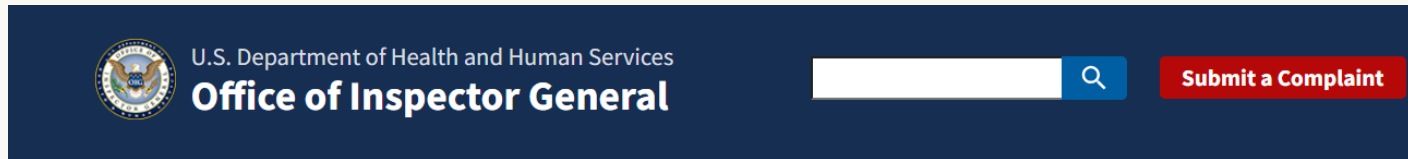
Disclaimer



- This is very brief and fast overview.
 - Alert you to issues and direct you to resources.
 - Not detailed analysis of the issues.
- May not cover all issues relevant to your organization.
- Remember state laws.

OIG General Compliance Guidance

<https://oig.hhs.gov/compliance/general-compliance-program-guidance/>



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 care compliance community and other health care stakeholders. The GCPG provides information about relevant Federal laws, compliance program infrastructure, OIG resources, and other information useful to understanding health care compliance.

The GCPG is voluntary guidance that discusses general compliance risks and compliance programs. The GCPG is not binding on any individual or entity. Of note, OIG uses the word "should" in the GCPG to present voluntary, nonbinding guidance.

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

[Download Complete Guidance](#)

[Individual Sections](#)



Nonbinding
but "should"

- 11/23: General Compliance Program Guidance
- 2024: Individual Segment-Specific Compliance Program Guidance
- Available on OIG website, <https://oig.hhs.gov/compliance/general-compliance-program-guidance/>

OIG General Compliance Program Guidance

Key Compliance Laws

1. Anti-Kickback Statute
2. Stark
3. False Claims Act
4. Civil Monetary Penalties Authorities
 - a. Beneficiary inducement
 - b. **Info Blocking**
 - c. **Grants, contracts, etc.**
5. Exclusions
6. Criminal Fraud
7. **HIPAA Privacy and Security**

Elements of Effective Compliance Program

1. Written policies and procedures
2. Compliance leadership and oversight
3. Training and education
4. Effective lines of communication with compliance officer and disclosure programs
5. Enforcing standards
6. **Risk assessment**, auditing and monitoring
7. Responding to detected offenses

➤ **Adaptions for small and large entities**

OIG General Compliance Program Guidance

Other Compliance Considerations

1. Quality and patient safety
2. New entrants into health care industry (e.g., tech, investors, non-traditional services)
3. Financial incentives: follow the money
 - a. Ownership, private equity, etc.
 - b. Payment incentives
4. Financial arrangement tracking

OIG resources

- Compliance toolkits, board resources, etc.
- OIG reports and publications
- Advisory opinions, fraud alerts, bulletins, etc.
- FAQs
- Corporate integrity agreements
- Enforcement action summaries
- OIG self-disclosure info
- OIG hotline

End of Public Health Emergency



PHE ended 5/11/23



Hospitals and CAHs (including Swing Beds, DPUs), ASCs and CMHCs: CMS Flexibilities to Fight COVID-19

At the beginning of the COVID-19 Public Health Emergency (PHE), CMS used emergency waiver authorities and various regulatory authorities to enable flexibilities so providers could rapidly respond to people impacted by COVID-19. CMS developed a cross-cutting initiative to use a comprehensive, streamlined approach to reestablish certain health and safety standards and other financial and program requirements at the eventual end of the COVID-19 public health emergency.

This CMS cross-cutting initiative focused on evaluating CMS-issued PHE waivers and flexibilities to prepare the health care system for operation after the PHE. This review happened in three concurrent phases:


1. CMS assessed the need for continuing certain waivers based on the current phase of the PHE. Since the beginning of the PHE, CMS has both added and terminated flexibilities and waivers as needed. In doing so, CMS considered the impacts on communities — including underserved communities — and the potential barriers and opportunities that the flexibilities may address.
2. CMS assessed which flexibilities would be most useful in a future PHE, such as natural and man-made disasters and other emergencies, to ensure a rapid response to future emergencies, both locally and nationally, or to address the unique needs of communities that may experience barriers to accessing health care.
3. CMS is continuing to collaborate with federal partners and the health care industry to ensure that the health care system is holistically prepared for addressing future

- COVID-19 vaccination requirements
- Reimbursement expansions
- Stark law waivers
- Telehealth flexibility
- Staff licensure
- Conditions of participation
- Discharge planning
- CAH bed count and length of stay
- ASC temporary hospital status
- Others

See <https://www.cms.gov/files/document/hospitals-and-cahs-ascs-and-cmhcs-cms-flexibilities-fight-covid-19.pdf>

Beware PHE fraud and abuse issues

*More about
fraud and
abuse issues
later...*

 DOJ Menu



Criminal Division
U.S. Department of Justice

[Our Offices](#) | [Find Help](#) | [Contact Us](#)

Search 

- [About](#) ▾
- [Leadership](#)
- [Press Room](#) ▾
- [Employment](#) ▾
- [FOIA](#) ▾
- [Resources](#)
- [Contact](#)

[Justice.gov](#) > [Criminal Division](#) > [About](#) > [Sections/Offices](#) > [Fraud Section](#) > [Health Care Fraud](#) > [Recent Enforcement Actions](#) > [2022 COVID-19 Enforcement Action](#) > Justice Department Announces Nationwide Coordinated Law Enforcement Action to Combat COVID-19 Health Care Fraud

**2022 COVID-19
Enforcement Action**

Case Summaries

[Court Documents](#)

[Press Release](#)

Justice Department Announces Nationwide Coordinated Law Enforcement Action to Combat COVID- 19 Health Care Fraud

[Share](#) >

Cybersecurity and Cyberthreats

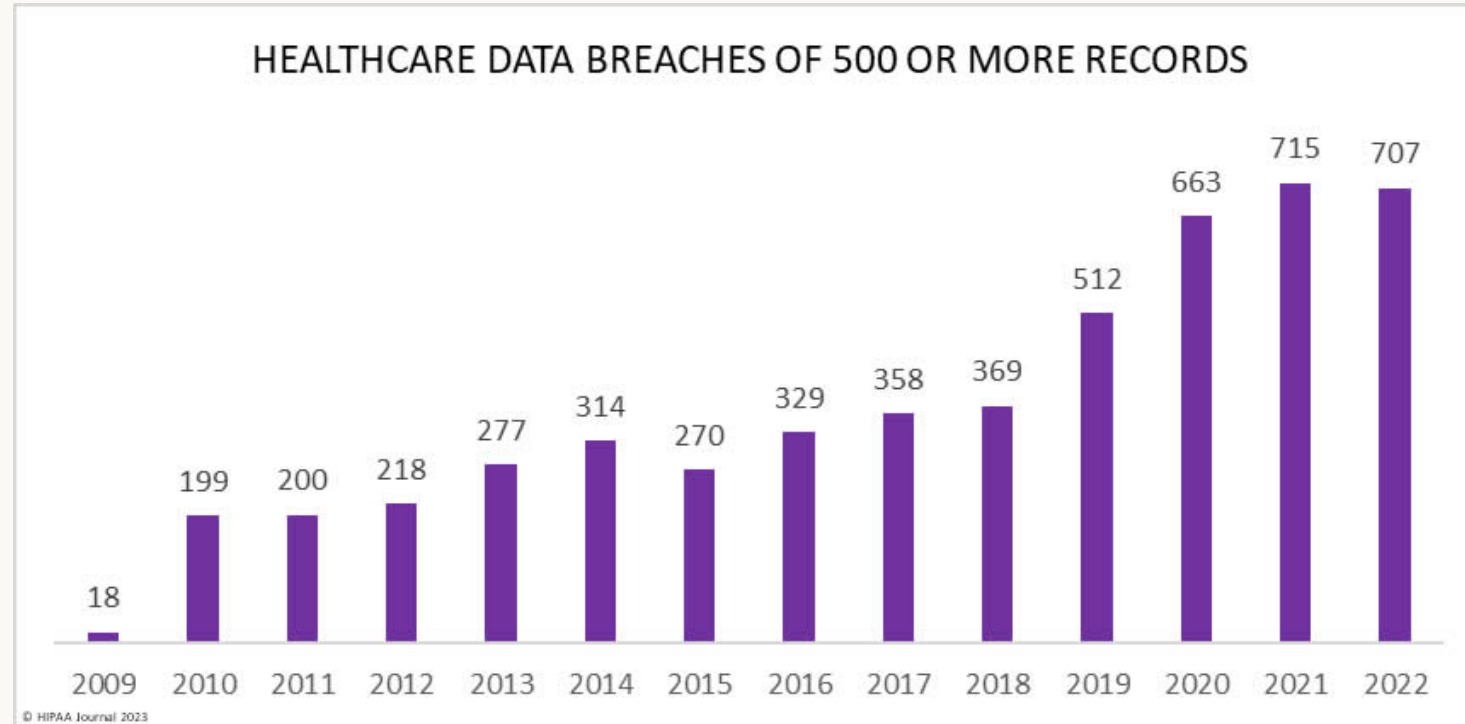
The other
pandemic



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/2022-healthcare-data-breach-report/>

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



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 Civil Penalties

Watch for new rule to 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">• \$127* to \$63,973* per violation• Up to \$1,919,173* 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">• \$1,280* to \$63,973* per violation• Up to \$1,919,173* 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">• \$12,794* to \$63,973* per violation• Up to \$1,919,173* per type per year• Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none">• \$63,973 to \$1,919,173* per violation• Up to \$1,919,173* per type per year• Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

HIPAA

Avoiding “Willful Neglect”

PRIVACY RULE

- May not access, use or disclose protected health info (PHI) without patient’s authorization or HIPAA exception.
- Implement safeguards.
- Train workforce members.
- Execute business associate agreements.
- Honor patient rights re PHI.
- Mitigate any breaches.
- Sanction employees.

(45 CFR 164.501 et seq.)

SECURITY RULE

- Perform and document periodic risk assessment.
- Implement safeguards.
 - Administrative
 - Technical, including encryption
 - Physical
- Execute business associate agreements.

(45 CFR 164.301 et seq.)

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

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 Rule requires that HIPAA-regulated entities must follow to protect the privacy and security of the information they create, receive, maintain, and transmit. The \$100,000 settlement resolves a large breach report regarding a ransomware attack that compromised 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. Victims are typically forced to pay the malware, until a ransom is paid. This marks the first ransomware settlement announced by OCR during Cybersecurity Awareness Month, and OCR has been working with the public to raise awareness of the threats in health care. In the past four years, there has been a 239% increase in ransomware threats covered by HIPAA to ensure better data security. Ransomware is a leading cause of data breaches in health care. In the past four years, there has been a 239% increase in ransomware threats involving hacking and a 278% increase in ransomware. This trend continues to be a significant concern, with 77% of the large breaches reported to OCR. Additionally, the large breaches reported this year have affected over 88 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

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 top of a TechTarget article. The header includes the TechTarget logo and 'HEALTH IT SECURITY | xtelligent HEALTHCARE MEDIA'. A navigation bar lists categories: HIPAA and Compliance, Cybersecurity, Cloud, Mobile, Patient Privacy, Data Breaches, and Disaster Preparedness. Below this is a banner for a white paper library about data encryption. The main headline reads 'Average Cost of Healthcare Data Breach Reaches \$11M'. The subtext states: 'The cost of a healthcare data breach has soared 53% since 2020, IBM's latest report revealed.' At the bottom, there is a blue button labeled 'Ponemon Institute'.

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.

OCR Cybersecurity Guidance

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

The screenshot shows the HHS website's HIPAA for Professionals section. At the top, there are four navigation buttons: "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". Below these, a breadcrumb trail reads: "HHS > HIPAA Home > For Professionals > The Security Rule > Security Rule Guidance Material > Cyber Security Guidance Material". A left-hand sidebar menu lists various topics: "HIPAA for Professionals", "Regulatory Initiatives", "Privacy", "Security" (which is expanded to show "Summary of the Security Rule", "Security Guidance", and "Cyber Security Guidance"), "Breach Notification", "Compliance & Enforcement", "Special Topics", "Patient Safety", and "Covered Entities & Business Associates". The main content area is titled "Cyber Security Guidance Material" and includes a sub-header "Cyber Security Checklist and Infographic". The text states: "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." Below this, there are two links: "Cyber Security Checklist - PDF" and "Cyber Security Infographic [GIF 802 KB]". Social media sharing icons for Twitter, Facebook, and Email are visible in the top right of the content area.

- 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_xaRWAC3qTYSykYAAbLL_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 (2023)

<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 [f](#) [t](#) [e](#)

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

24

 Holland & Hart

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 engineering¹ that hackers use to gain access to healthcare information systems and data.² 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>

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>)

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 consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

Cases

- [Epic Games, In the Matter of](#) (September 19, 2023)
- [1Health.io/Vitagene, In the Matter of](#) (September 7, 2023)
- [Edmodo, LLC, U.S. v.](#) (August 28, 2023)
- [Amazon.com \(Alexa\), U.S. v.](#) (July 21, 2023)
- [BetterHelp, Inc., In the Matter of](#) (July 14, 2023)
- [Facebook, Inc., In the Matter of](#) (July 13, 2023)
- [Easy Healthcare Corporation, U.S. v.](#) (June 26, 2023)
- [Microsoft Corporation, U.S. v.](#) (June 9, 2023)
- [Ring, LLC](#) (May 31, 2023)
- [GoodRx Holdings, Inc.](#) (February 17, 2023)
- [Epic Games, Inc., U.S. v.](#) (February 7, 2023)
- [Chegg](#) (January 26, 2023)
- [Drizly, LLC., In the Matter of](#) (January 10, 2023)
- [FTC v Kochava, Inc.](#) (August 29, 2022)
- [CafePress, In the Matter of](#) (June 24, 2022)

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 U.S. Securities and Exchange Commission (SEC) website. The header includes the SEC logo, the text "U.S. SECURITIES AND EXCHANGE COMMISSION", a search bar labeled "Search SEC.gov", and a link to "COMPANY FILINGS". A dark blue navigation bar contains links for "ABOUT", "DIVISIONS & OFFICES", "ENFORCEMENT", "REGULATION", "EDUCATION", "FILINGS", and "NEWS". On the left, a "Newsroom" sidebar lists "Press Releases" (highlighted), "Speeches and Statements", "SEC Stories", "Securities Topics", "Media Kit", "Press Contacts", "Events", "Webcasts", and "Media Gallery", with an "RSS Feeds" link at the bottom. The main content area features a "Press Release" title with social media icons. The headline is "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies". Below the headline, it says "FOR IMMEDIATE RELEASE 2023-139". The text of the release begins with "Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures." A quote from SEC Chair Gary Gensler follows: "Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," said SEC Chair Gary Gensler. "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them." To the right of the headline, a "Related Materials" section lists "Final Rule" and "Fact Sheet".

HIPAA and Data Privacy



Recent HIPAA Settlements

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

Date	Conduct	Settlement
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 requirements.	\$1,250,000
1/23/23	Life Hope Labs failed to provide personal rep with records of deceased patient.	\$16,500
9/20/22 ²⁹	Great Expressions Dental failed to provide records and charged more than reasonable fee.	\$80,000

HIPAA Privacy Rule: Right of Access

U.S. Department of Health and Human Services
Enhancing the health and well-being of all Americans

Home > About > News > UnitedHealthcare Pays \$80,000 Settlement to HHS to Resolve HIPAA Matter over Patient Medical Records Request

FOR IMMEDIATE RELEASE
August 24, 2023

Contact: HHS Press Office
202-690-6343
media@hhs.gov

UnitedHealthcare Pays \$80,000 Settlement to HHS to Resolve HIPAA Matter over Patient Medical Records Request

OCR settles forty-fifth HIPAA Right of Access investigation

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has announced a

OCR's 45th settlement over access.

- Ensure you timely respond to patient's or personal rep's request to access records.
 - Applies to records in designated record set.
 - Limited exceptions.
 - Includes records from other providers.
 - 30-day / 60-day time limit.
 - Beware Info Blocking Rule implications.
 - 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. 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.

OCR and FTC Warn Against Data Tracking Technologies

<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 Asso...

HIPAA for Professionals	
Regulatory Initiatives	
Privacy	+
Security	+
Breach Notification	+
Compliance & Enforcement	+
Special Topics	+
Patient Safety	+
Covered Entities & Business Associates	+
Training & Resources	
FAQs for Professionals	
Other Administrative Simplification	

T+

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

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities¹ and business associates² (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”).³ OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about noncompliance with the HIPAA Rules. A regulated entity’s failure to comply with the HIPAA Rules may result in a civil money penalty.⁴

Tracking technologies are used to collect and analyze information about how users interact with regulated entities’ websites or mobile applications (“apps”). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity’s health care operations.⁵ The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors

12/1/22

7/20/23



July 20, 2023

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

Re: Use of Online Tracking Technologies
Dear [Name of Recipient],

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

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

¹See, e.g., Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers’ Exfiltration of PHI from Healthcare Providers’ Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), <https://dl.acm.org/doi/10.1145/3559613.3563190>.
²See, e.g., Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.
³*U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023-186-easy-healthcare-corporation-privacy-breach>; *Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc>; *Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-go-health-inc>; *Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-betterhelp-inc>.
⁴U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

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 security, you've probably thought about the Health Insurance Portability and Accountability Act of

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.

(See <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

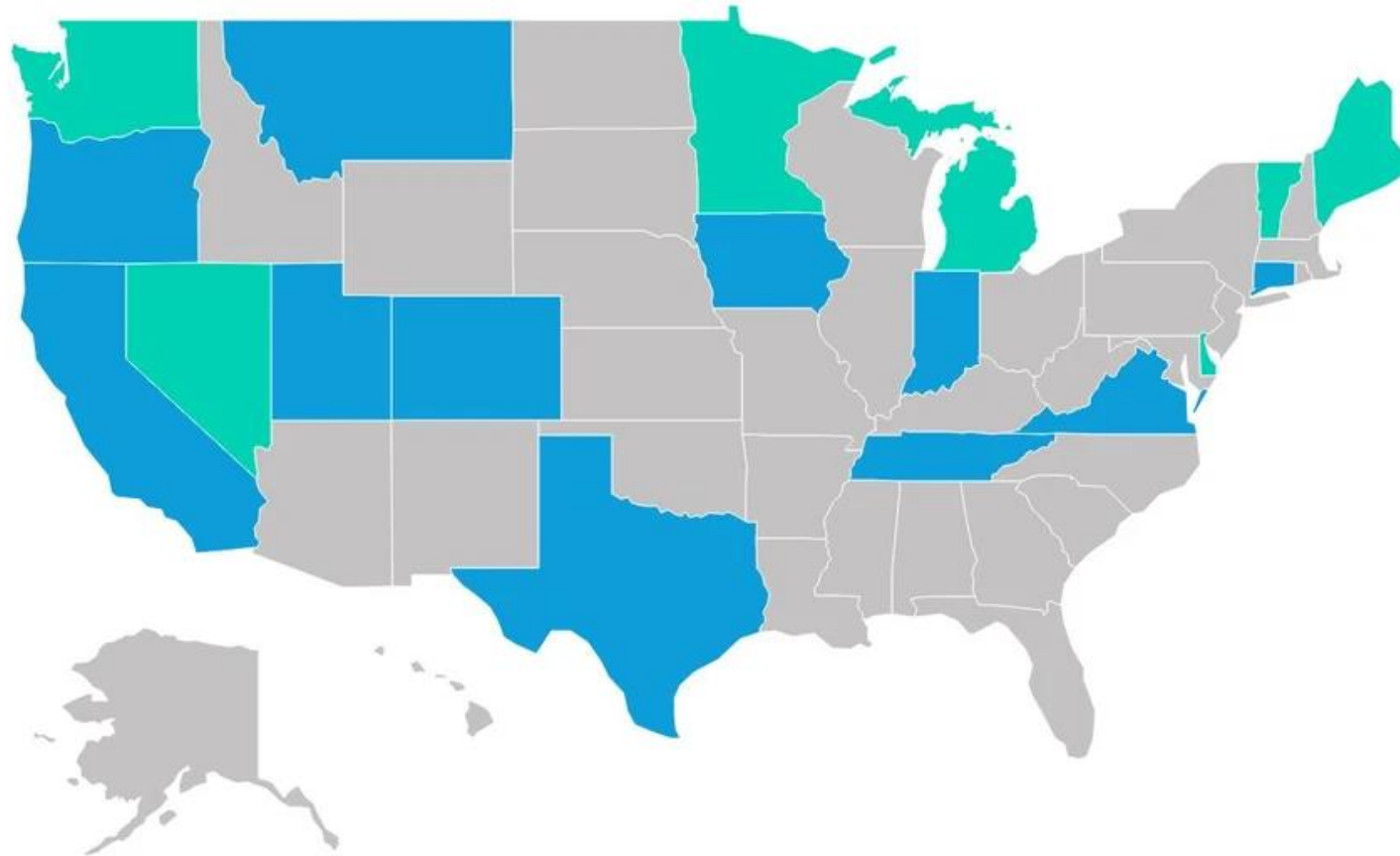
- Strengthened individual's right of access.
 - Allows individuals to take notes or use other personal devices to view and capture images of PHI.
 - Must respond to requests to access within 15 days.
 - Requires providers to share info when directed by patient.
 - Further limits charges for producing 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))

Other Privacy and Security Developments

- SAMHSA has proposed changes to Part 2 rules to align with HIPAA (87 FR 74216 (12/2/22))
- Health Information Breach Notification Rule (16 CFR part 316)
 - Applies to vendors of personal health info.
 - Not entities covered by HIPAA (covered entities and business associates)
 - FTC proposed rule strengthens HBNR (88 FR 37819 (6/9/23))
 - FTC actively enforcing Health Information Breach Notification Rules
 - GoodRx pays \$1.5 million

States Enacting Data Privacy Laws



● Comprehensive privacy law ● Narrow privacy law ● Other applicable law

As of 9/7/23

See

<https://pro.bloomberglaw.com/brief/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
- 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

Proposed Rule 21st 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)



Hart

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)



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>



TOPICS ▾

BLOG

NEWS ▾

DATA

ABOUT ONC ▾



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

Information Blocking

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



Fraud and Abuse



- False Claims Act
- Anti-Kickback Statute (AKS)
- Eliminating Kickback in Recovery Act (EKRA)
- Ethics in Patient Referrals Act (Stark)
- Civil Monetary Penalties Law (CMPL)

Anti-Kickback Statute (AKS)

- Cannot knowingly and willfully offer, pay, solicit or receive remuneration to induce referrals for items or services covered by government program unless transaction fits within a regulatory safe harbor.

(42 USC 1320a-7b(b); 42 CFR 1003.300(d))

- "One purpose" test

(*US v. Greber*, 760 F.2d 68 (1985))

Penalties

- Felony
 - 10 years in prison
 - \$100,000 criminal fine
- \$112,131* civil penalty
- 3x damages
- Exclusion from Medicare/Medicaid
(42 USC 1320a-7b(b); 42 CFR 1003.310; 45 CFR 102.3)
- False Claims Act violation
 - Must report and repay
 - \$11,803 to \$23,607 per claim
 - Qui tam lawsuits

(42 USC 1320a-7a(a); 42 CFR 1003.210; 45 CFR 102.3)

- Minimum \$100,000 settlement through self-disclosure protocol.

AKS: Physician Wellness Safe Harbor

- In 12/22, CCA 2023 enacted new AKS exception for physician wellness programs.
 - Hospitals, ASCs, SNFs and certain other entities may offer a bona fide mental health or behavioral health improvement or maintenance program to physicians who practice in the area serviced by the facility.
 - Effective for programs after 12/29/22.

(42 USC 1320a-7b(b)(3))
- *Don't forget about 2021 AKS safe harbors, including value-based enterprise safe harbors.*

AKS: Frequently Asked Questions

- OIG FAQs re Fraud and Abuse Authorities, <https://oig.hhs.gov/faqs/general-questions-regarding-certain-fraud-and-abuse-authorities/>
 - Effect of failure to fit safe harbor
 - AKS v. CMPL v. Stark
 - Cash, cash equivalents, and “in-kind” gift cards
 - AKS and EHR vendors
 - Referrals between entities with common ownership
 - ASC safe harbor
 - Inflation caps
 - PBMs
 - Others

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

Search:

About OIG ▾ Reports ▾ Fraud ▾ Compliance ▾ Exclusions ▾ Newsroom ▾ Careers ▾ COVID-19 Portal

[Home](#) > [Frequently Asked Questions](#) > General Questions Regarding Certain Fraud and Abuse Authorities

General Questions Regarding Certain Fraud and Abuse Authorities

(1) When an arrangement does not satisfy a safe harbor under the Federal anti-kickback statute, does that mean it's automatically illegal? If an arrangement satisfies most of a safe harbor's conditions, does that mean it is lower risk?

The safe harbor regulations at 42 CFR § 1001.952 describe various payment and business practices that, although they potentially implicate the Federal anti-kickback statute, are not treated as offenses under the statute. Compliance with a safe harbor is voluntary; failure to satisfy a safe harbor does not mean that an arrangement is illegal.

There is no safe harbor protection for partial compliance with the conditions of a potentially applicable safe harbor. To receive the benefit of safe harbor protection, an arrangement must squarely satisfy

Eliminating Kickback in Recovery Act (EKRA)



- Cannot solicit, receive, pay or offer any remuneration in return for referring a patient to a laboratory, recovery homes or clinical treatment facility unless arrangement fits within regulatory exception.
(18 USC 220(a))
- Applies to referrals paid by private or public payers.

Penalties

- \$200,000 criminal fine
- 10 years in prison
(18 USC 220(a))

Beware:

- Few statutory safe harbors.
- No regulatory safe harbors.
- Cases suggest DOJ may interpret and apply EKRA broadly to combat fraud and abuse in labs. (See, e.g., *US v. Schena* (N.D. Cal. 2022); *S&G Labs Hawaii v. Graves* (D. Haw. 2021))

Ethics in Patient Referrals Act (Stark)

- If physician (or family member) has financial relationship with entity:
 - Physician may not refer patients to entity for designated health services (DHS), and
 - Entity may not bill Medicare or Medicaid for such DHS unless arrangement fits within a regulatory exception.

(42 USC 1395nn; 42 CFR 411.353 and 1003.300)

Penalties

- No payment for services provided per improper referral.
 - Repayment w/in 60 days.
 - Civil penalties.
 - \$27,750* per claim submitted
 - \$174,172* per scheme
- (42 CFR 411.353, 1003.310; 45 CFR 102.3)

Beware

- Strict liability statute.
- Likely False Claims Act violation
- Likely Anti-Kickback Statute violation

Stark: CMS Clearing Backlog of SRDP

- Settlements are small % of potential exposure.
- Recent Stark changes have made it easier to comply and withdraw from SRDP.
- Changes to SRDP effective 3/1/23

Self-Referral Disclosure Protocol Settlements

The CMS Voluntary Self-Referral Disclosure Protocol (SRDP) enables providers of services and suppliers to self-disclose actual or potential violations of the physician self-referral statute. The following table displays settlements to date and will be updated on a yearly basis.

Calendar Year	Number of Disclosures Settled	Range of Amounts of Settlements	Aggregate Amount of Settlements
2011	3	\$60 - \$579,000	\$709,060
2020	36	\$33 - \$952,300	\$4,344,966
2021	27	\$631 - \$1,110,148	\$1,988,451
2022	104	\$299 - \$1,171,174	\$9,287,866
Totals	502	\$33 - \$1,196,188	\$47,444,700

As of December 31, 2022, an additional 232 disclosures to the SRDP were withdrawn, closed without settlement or settled by CMS' law enforcement partners.

confidentially, on an aggregate basis.

Feedback

Stark: Recent Developments

- In 12/22, CCA 2023 enacted new Stark exception for physician wellness programs.
 - Hospitals, ASCs, SNFs and certain other entities may offer a bona fide mental health or behavioral health improvement or maintenance program to physicians who practice in the area serviced by the facility.
 - Effective for programs after 12/29/22.

(42 USC 1395nn(e)(9))
- Effective 10/1/23, CMS modifies process for requesting exception for physician-owned hospital expansions. (<https://www.cms.gov/medicare/regulations-guidance/physician-self-referral/spotlight>)
- *Review 2021 Stark changes, including value-based enterprise safe harbors.*

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, e.g.,
 - Conditions of payment
 - Anti-Kickback Statute and Stark
- 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 monetary penalties of \$11,803* to \$23,607* per claim
 - Admin penalty \$22,427* per claim failed to return
 - 3x damages
 - Exclusion from Medicare/Medicaid
- (42 USC 1320a-7a(a); 42 CFR 1003.210; 45 CFR 102.3; 86 FR 70740)
- Potential *qui tam* lawsuits

False Claims Act: Application

- Former VP brought qui tam action claiming health system violated FCA, AKS, and Stark:
 - Medical directorships > fair market value
 - Provide free PAs, billing, and admin support to referring physicians, including free support to help physicians catch up on documentation.
 - Paying overhead costs of referring physicians.
 - Billing Medicare/Medicaid for services provided without supervisory physicians onsite.
 - No oversight and no records maintained to justify compensation.
- Settled for \$69 million



False Claims Act: Penalties



Office of Public Affairs
U.S. Department of Justice

[Our Offices](#) | [Find Help](#) | [Contact Us](#)

[About](#)[News](#)[Documents](#)[Internships](#)[FOIA](#)[Contact](#)[Information for Journalists](#)

[Justice.gov](#) > [Office of Public Affairs](#) > [News](#) > [Press Releases](#) > [False Claims Act Settlements and Judgments Exceed \\$2 Billion In Fiscal Year 2022](#)

News

[All News](#)[Blogs](#)[Photo Galleries](#)

PRESS RELEASE

False Claims Act Settlements and Judgments Exceed \$2 Billion in Fiscal Year 2022

False Claims Act Developments

- FCA liability requires that the defendant act “knowingly,” i.e.,
 - Actual knowledge
 - Deliberate ignorance
 - Reckless disregard of the truth or falsity, including substantial and unjustifiable risk of falsity.
- Depends on plaintiff’s knowledge and subjective belief.
 - Cannot avoid liability by establishing objectively reasonable interpretation of ambiguous law.

(US ex rel. Schutte v. SuperValue, Inc. (S.Ct. 2023))

Recent OIG Self-Disclosures

<https://oig.hhs.gov/fraud/enforcement/?type=fraud-self-disclosures>

Date	Alleged Conduct	Amount
9/28/23	Baptist Medical Center knowingly retained overpayments .	\$131,000
9/20/23	Brickyard Healthcare submitted claims for services provided by unlicensed person .	\$35,000
9/14/23	Advanced Garden State Cardiology employed excluded individual and submitted claims by unlicensed and excluded individual.	\$159,000
9/8/23	Missouri Healthcare System submitted claims for services that failed to meet standards of care or were medically unnecessary .	\$619,000
8/17/23	IvyRehab paid remuneration to physicians through discounts and waived patient cost-sharing obligations .	\$171,000
8/3/23	Tarpon Interventional Spine submitted claims for services that misidentified rendering provider .	\$21,000
7/21/23	Team Rehab Services submitted claims for services that were not reimbursable and did not meet requirements for time-based codes.	\$12,200,000
6/29/23	Ascension St. Vincent's Birmingham paid remuneration in form of free office space .	\$100,000

Advisory Opinions

AKS and CMPL

The screenshot shows the homepage of the U.S. Department of Health and Human Services Office of Inspector General. The header includes the department name and a search bar. The main navigation menu includes links for About OIG, Reports, Fraud, Compliance, Exclusions, Newsroom, Careers, and a COVID-19 Portal. The breadcrumb trail reads: Home > Compliance > Advisory Opinions. The main heading is "Advisory Opinions". Below it, a paragraph states: "HHS-OIG issues advisory opinions about the application of certain fraud and abuse enforcement authorities to the requesting party's existing or proposed business arrangements." A button labeled "View All Opinions" is present. At the bottom, there is a search bar with the placeholder text "Search opinions" and a "Search" button. A taskbar with various application icons is visible at the very bottom of the browser window.

Stark

The screenshot shows the CMS.gov website, specifically the "Advisory Opinions (AOs)" page. The header includes the CMS.gov logo and the text "Centers for Medicare & Medicaid Services". The main navigation menu includes links for Medicare, Medicaid/CHIP, Marketplace & Private Insurance, Priorities, and Training & Education. The breadcrumb trail reads: Home > Medicare > Regulations & guidance > Physician Self Referral > Advisory Opinions (AOs). The main heading is "Advisory Opinions (AOs)". Below it, a paragraph states: "Section 1877(g)(6) of the Social Security Act (the Act) requires that CMS issue certain written advisory opinions. These opinions provide guidance on whether a physician's referrals for certain designated health services payable by Medicare to an entity with which he or she (or an immediate family member) has a financial relationship are prohibited under the Medicare program by section 1877 of the Act. We are making these advisory opinions available to the general public through this CMS website, as specified in our regulations at 42 CFR 411.384(b). The purpose of the advisory opinion process is to provide a binding opinion concerning the application of section 1877 of the Act to specific factual situations." Another paragraph states: "The requestor, who must be a party to the existing or proposed arrangement, is the only individual or entity that may rely on the advisory opinion. In each opinion, we apply legal standards to a set of facts involving certain known persons and/or entities that have provided specific statements about key factual issues. Because each opinion applies to specific individuals or entities in specific situations, no third parties are bound by, nor may they legally rely on, an advisory opinion." A taskbar with various application icons is visible at the very bottom of the browser window.

- May request AO.
- AOs are not binding on others but provide helpful guidance.

Common State Laws and Regulations

- False claims acts
- Anti-kickback statutes
- Self-referral prohibitions
- Fee splitting prohibition
- Disclosure of financial interests
- Insurance statutes
- Medicaid conditions
- Fraud or misrepresentation
- Consumer protection laws
- Bribery (may trigger federal Travel Act claims)
- Others?

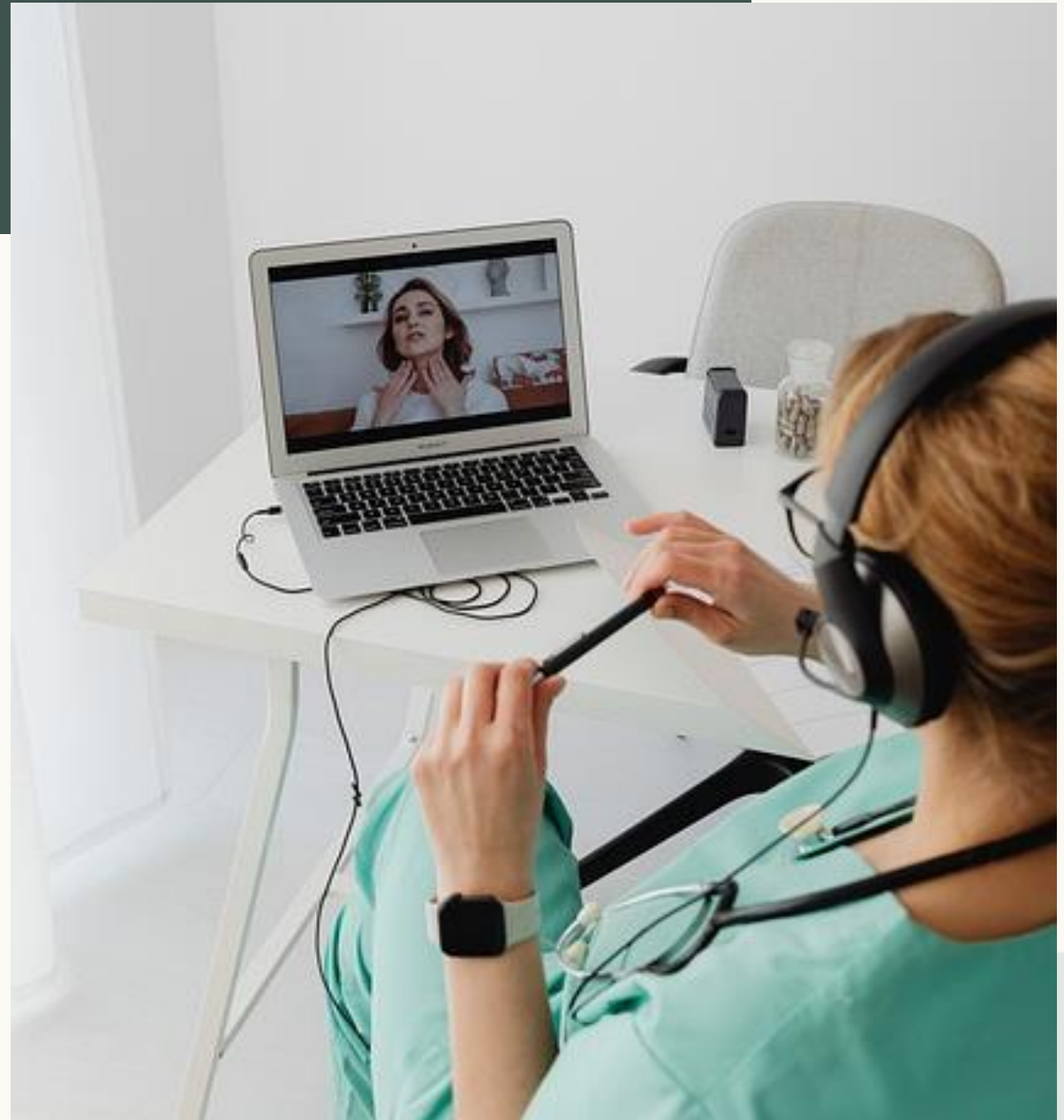
Penalties

- Civil penalties
- Criminal penalties
- Adverse licensure action
- Other

Beware

- *May apply to private payers in addition to govt programs.*
- *May not contain the same exceptions or safe harbors as federal statutes.*

Telehealth



Telehealth

- Most PHE waivers or relaxed standards have ended, e.g.,
 - Licensure rules
 - HIPAA security rules for platforms
 - Electronic prescribing
 - Location for services
 - Payer reimbursement requirements
- But Medicare has extended or retained some changes, especially for behavioral health.



Check relevant
state law

Beware Applicable Law

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
- Malpractice liability and insurance
- Corporate practice of medicine
- Others?

Ryan Haight Online Pharmacy Consumer Protection Act

- Prohibits providers from prescribing controlled substances via the internet without having previously performed an in-person medical evaluation of the patient.
- Exceptions:
 - Prescribing provider is temporarily covering for another provider with a treatment relationship; or
 - Patient being treated in DEA-registered facility, provider has DEA registration in state in which patient is located, and provider renders telehealth through 2-way interactive audio and video communication system.

(21 USC 829; 21 CFR 1306.09)

Ryan Haight Act: Remote Prescribing

- In 2/23, DEA issued proposed rules that would modify the regulations for remote prescribing.
- In meantime, DEA has issued temporary rules extending COVID-19 PHE flexibilities through 12/31/24.
 - Registered practitioner may prescribe schedule II–V controlled substances via telemedicine to a patient without having in-person medical evaluation if:
 - The prescription is issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice;
 - The prescription is issued pursuant to a communication between a practitioner and a patient using an interactive telecommunications system satisfying certain conditions;
 - The prescription is consistent with all other requirements of 21 CFR part 1306.

(21 CFR 1307.41; 88 FR 69879 (10/10/23))

Ryan Haight Act: Remote Prescribing

- DEA proposed rule would allow telehealth prescription without in-person evaluation for:
 - 30-day supply of Schedule III-V non-narcotic controlled medications; and
 - 30-day supply of buprenorphine for treatment of opioid use disorder.

(88 FR 12875; <https://www.dea.gov/press-releases/2023/02/24/dea-announces-proposed-rules-permanent-telemedicine-flexibilities>)

SUPPORT Act

- Facilitates telehealth for substance use disorders (SUD) by:
 - DEA required to establish a telehealth registration process to facilitate prescriptions for SUD.
 - See new proposed rule
 - State Medicaid programs required to allow for prescription of controlled substances to SUD patients via telehealth.
 - Medicare beneficiaries allowed to receive telehealth in their home.
 - Home is an approved “originating site”.

(21 USC 831(h)(2) and 42 USC 1395m and 1396a)

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
- 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 /](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 pose risks to national security. Harnessing AI for good and realizing its

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.

Artificial Intelligence: Compliance Considerations

- Privacy of data input to AI
 - HIPAA (e.g., use of de-identified PHI, permissible use, etc.)
 - 42 CFR part 2
 - FTCA § 5
 - State laws
- Unlicensed practice of medicine
 - Licensed provider must retain ultimate decision-making authority
- Malpractice
 - Reliance on AI may be inconsistent with applicable standard of care
- Billing compliance
 - AI may not incorporate all applicable regulations or payer requirements.

Artificial Intelligence: Compliance Considerations

- Anti-Kickback Statute or other fraud and abuse concerns
 - Incorrect or false claims.
 - Improper inducements, e.g., AI developer builds AI in a manner that recommends a particular item or service payable by federal healthcare programs. (See 88 FR 23777 (4/18/23); OIG FAQs, <https://oig.hhs.gov/faqs/general-questions-regarding-certain-fraud-and-abuse-authorities/>)
- Anti-Discrimination laws
 - AI may result in prohibited discrimination against persons. (See DOJ, EEOC, FTC *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems* (6/3/23), https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf)
 - HHS proposed 1557 rule prohibits discrimination “through use of clinical algorithms in its decisionmaking.” (87 FR 47914 (8/4/22))

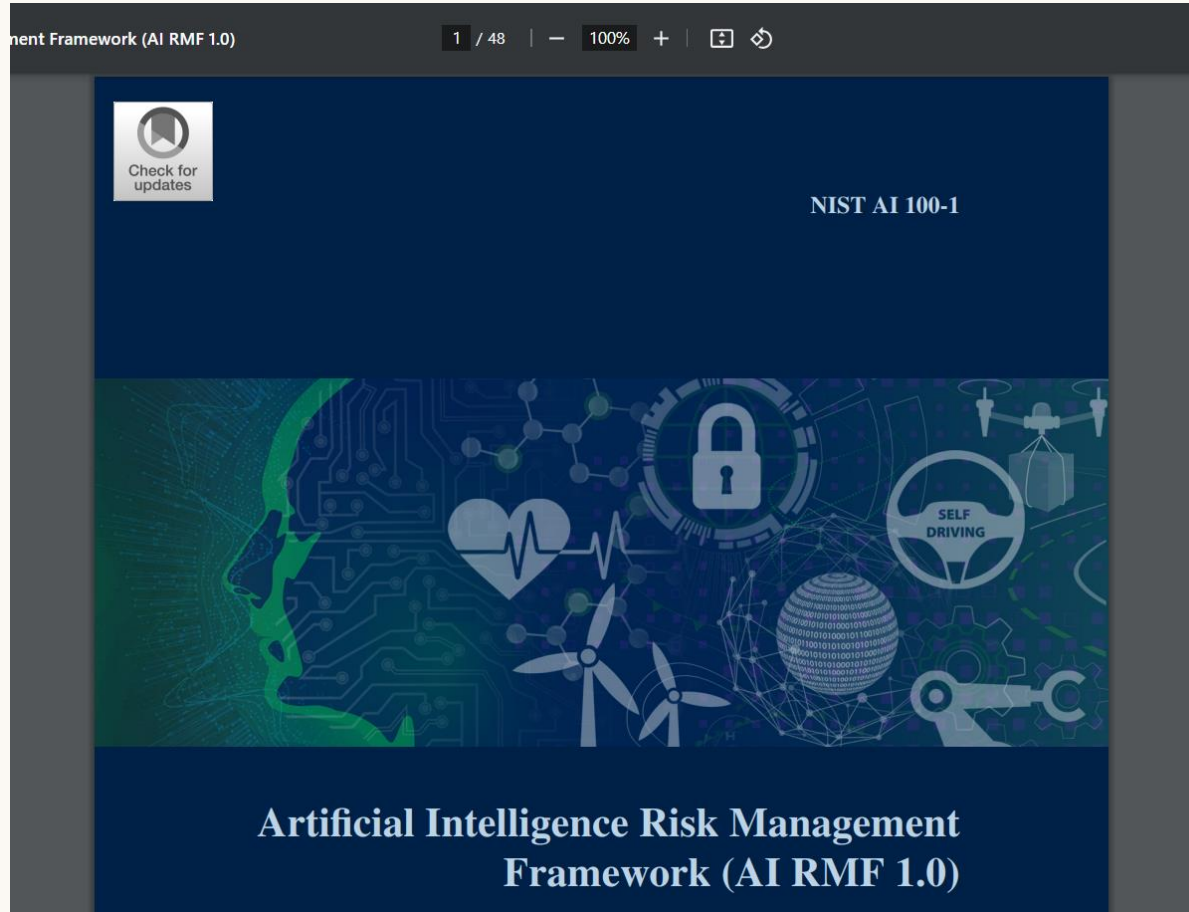
Artificial Intelligence: Compliance Considerations

- FDA Regulation of Devices
 - Cures Act amended FDCA to exclude certain software functions from device if satisfy criteria, generally including that the software is:
 - Not intended to analyze certain info;
 - Intended to support or provide recommendations to treating clinician; and
 - Intended to enable clinician to independently review basis of software recommendations so clinician does not rely primarily on software's recommendation to diagnose or treat patient.
(See 21 USC 360j(o))
 - FDA rules exclude certain software functions from definition of "device" regulated by FDA. (86 FR 20278 (4/19/21))
- Electronic health record certification
 - In 4/23, ONC issued proposed rule (HTI-1) for certified health technologies to increase trust in predictive technologies. (88 FR 23746 (4/18/23))
 - May serve as basis for legislation in other contexts.

AI may
be
"device"

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

AMA Policy re Augmented Intelligence in Healthcare

<https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf>

- AI enhances human intelligence rather than replaces it.
- Requires oversight and regulation considering benefit and risk of harm.
- Payment and coverage must be practical and advance affordability.
- Use should not be mandated.
- Liability and incentives aligned, with developers accountable.



Policy

The American Medical Association House of Delegates has adopted policies to keep the focus on advancing the role of augmented intelligence (AI) in enhancing patient care, improving population health, reducing overall costs, increasing value and the support of professional satisfaction for physicians.

Foundational policy Annual 2018

As a leader in American medicine, our AMA has a unique opportunity to ensure that the evolution of AI in medicine benefits patients, physicians and the health care community. To that end our AMA seeks to:

- Leverage ongoing engagement in digital health and other priority areas for improving patient outcomes and physician professional satisfaction to help set priorities for health care AI
- Identify opportunities to integrate practicing physicians' perspectives into the development, design, validation and implementation of health care AI
- Promote development of thoughtfully designed, high-quality, clinically validated health care AI that:
 - Is designed and evaluated in keeping with best practices in user-centered design, particularly for physicians and other members of the health care team
 - Is transparent
 - Conforms to leading standards for reproducibility
 - Identifies and takes steps to address bias and avoids introducing or exacerbating health care disparities, including when testing or deploying new AI tools on vulnerable populations

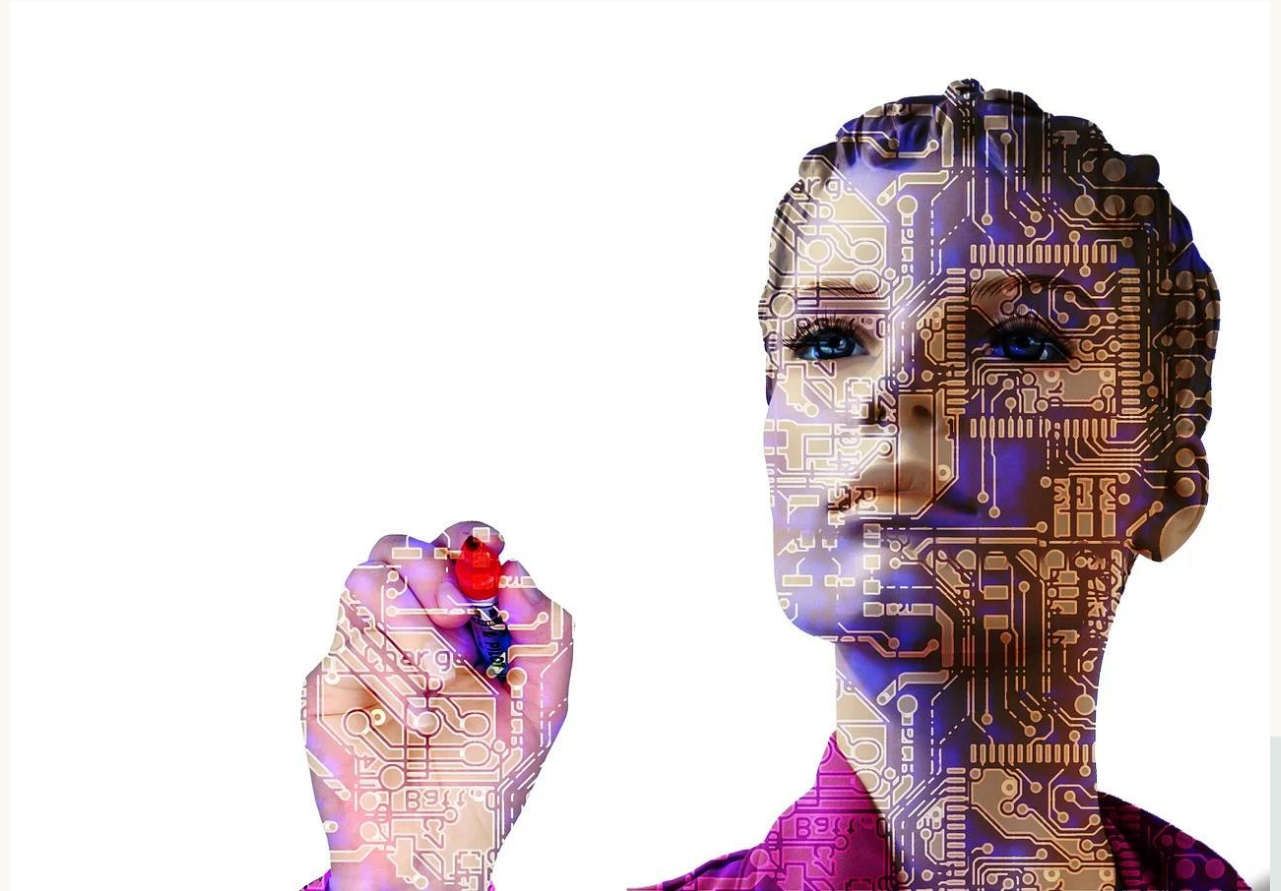
“Medical experts are working to determine the clinical applications of AI—work that will guide health care in the future. These experts, along with physicians, state and federal officials must find the path that ends with better outcomes for patients. We have to make sure the technology does not get ahead of our humanity and creativity as physicians.”

—Gerald E. Harmon, MD, AMA Board of Trustees

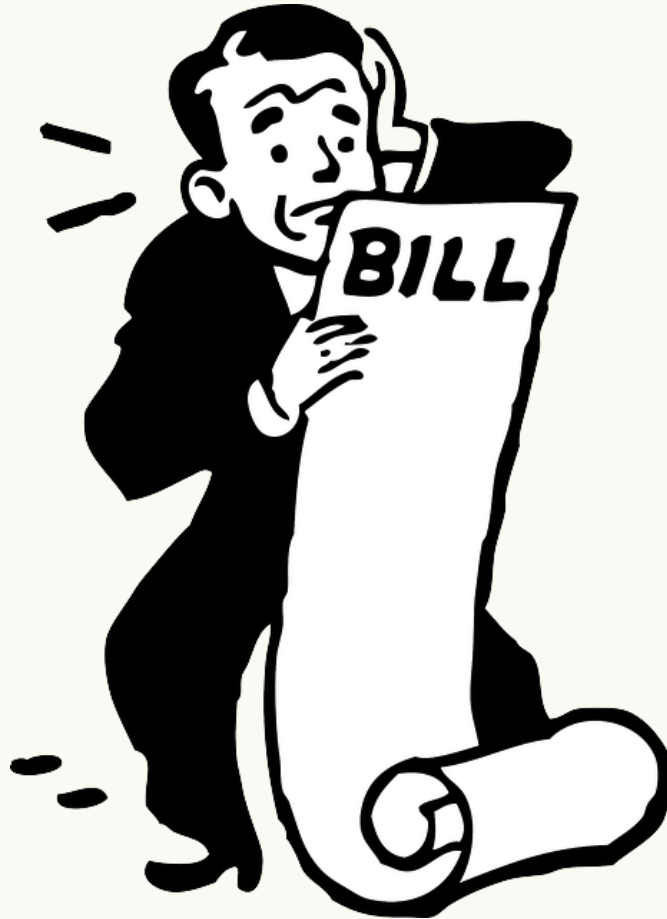
- Safeguards patients' and other individuals' privacy interests and preserves the security and integrity of personal information
- Encourage education for patients, physicians, medical students, other health care professionals and health administrators to promote greater understanding of the promise and limitations of health care AI
- Explore the legal implications of health care AI, such as issues of liability or intellectual property, and advocate for appropriate professional and governmental oversight for safe, effective, and equitable use of and access to health care AI

Artificial Intelligence

- Stay tuned as the law attempts to catch up...
 - Federal laws and regulations
 - State laws and regulations
 - Industry standards and reliability
- In the meantime, beware its limitations and risks under the current framework.



No Surprise Billing Rules



No Surprise Billing Rules

INSURED PATIENTS

- Limits amount out of network (OON) provider/facility may bill patient and payer.
- Only applies to:
 - Hospital or freestanding emergency dept.
 - Hospital, hospital outpatient dept, or ASC.
- Independent dispute resolution (IDR) process to resolve disputes about charges.

(45 CFR 149.410-.450)

SELF-PAY PATIENTS

- Providers/facilities must:
 - Post notices.
 - Give patient a good faith estimate of charges.
 - **Co-Provider Rules Postponed.**
 - See forms at <https://www.cms.gov/nosurprises/policies-and-resources/overview-of-rules-fact-sheets>)
- Patient-provider dispute resolution (PPDR) process if actual bill is substantially in excess (i.e., > \$400) of good faith estimate.
(45 CFR 149.610-.620)

No Surprise Billing Rules Developments

- Texas federal district court has repeatedly struck down govt application of qualifying payment amount (QPA), IDR process, and fees. (*Texas Medical Ass'n v. HHS* (E.D. Tex. 2022))
 - Litigation ongoing.
- Govt has proposed new rule addressing IDR process. (88 FR 65888 (9/26/23))
- Govt suspended IDR process for a time but has resumed individual claims on 10/6/23. (<https://www.cms.gov/files/document/federal-idr-partial-reopening-faqs-oct-23.pdf>)
- Govt has issued FAQs addressing No Surprise Billing Rules and IDR process. (<https://www.cms.gov/files/document/federal-idr-partial-reopening-faqs-oct-23.pdf>)

FAQs re Reopening IDR Process

<https://www.cms.gov/files/document/federal-idr-partial-reopening-faqs-oct-23.pdf>

Federal Independent Dispute Resolution (IDR) Process Partial Reopening of Dispute Initiation Guidance

October 2023

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.



- For individual disputes:
 - Provides limited grace period for initiating IDRs.
 - Check deadlines for pending IDRs.
- For batched disputes:
 - Watch for future guidance.

CMS Updates re IDR Process



Centers for Medicare & Medicaid Services

[About CMS](#) [Newsroom](#) [Data & Research](#)



[Medicare](#) ▾

[Medicaid/CHIP](#) ▾

[Marketplace & Private Insurance](#) ▾

[Priorities](#) ▾

[Training & Education](#) ▾

[Home](#) > [Priorities](#) > [Recent Legislation](#) > [No Surprises Act](#) > [Payment disputes between providers and health plans](#)

[Home](#)

[Policies & Resources](#) ▾

[Resolving out-of-network payment disputes](#) ▾

[Consumers and Advocates](#) ▾

Payment disputes between providers and health plans

Notices

November 1, 2023


The Departments are working to re-open the Federal IDR portal for all batched disputes and single air ambulance disputes. The Departments are aware that disputing parties are actively making decisions about whether to initiate disputes as single disputes for items and services that may subsequently be eligible for submission as a batched dispute once the portal is re-opened for batched disputes. As with prior portal re-opening announcements, the Departments will extend initiation deadlines to allow parties additional time to initiate batched and air ambulance disputes involving items and services for which the IDR initiation period ended during the time that batched and air ambulance dispute initiation was unavailable.

October 6, 2023


Feedback

CMS Website re No Surprise Billing


<https://www.cms.gov/nosurprises>

 Centers for Medicare & Medicaid Services

About CMSNewsroomData & Research



Medicare ▾Medicaid/CHIP ▾Marketplace & Private Insurance ▾Priorities ▾Training & Education ▾


 > Priorities > Recent Legislation > No Surprises Act

HomePolicies & Resources ▾Resolving out-of-network payment disputes ▾Consumers

Effective October 6, 2023, the Departments have reopened the Federal IDR portal for the initiation of certain new single and bundled disputes. Processing and initiation of batched disputes and initiation of new air ambulance disputes remains temporarily suspended. The Departments are conducting a phased reopening of the portal and will make additional announcements regarding other suspended dispute categories soon.

Ending Surprise Medical Bills

Learn how providers, facilities, plans and issuers can comply with surprise billing protections and resolve out-of-network



Hospital Price Transparency Rules



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-oppsasc-final-rule-increases-price-transparency-patient-safety-and-access-quality-care>)

Price Transparency: Enforcement

Hospital price transparency

Enforcement actions

- 14 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 with the 'Hospital Price Transparency' section highlighted. The page features a navigation bar with links to Home, About CMS, Newsroom, Archive, Help, and Print. Below the navigation bar is a search bar and a row of yellow buttons for various CMS services. The main content area has a dark blue header with the text 'Hospital Price Transparency' and a large white dollar sign icon. Below this, a dark blue box contains text explaining the purpose of hospital price transparency and listing two ways hospitals will provide pricing information.

Home | About CMS | Newsroom | Archive | Help | Print

CMS.gov
Centers for Medicare & Medicaid Services

Search CMS Search

Medicare Medicaid/CHIP Medicare-Medicaid Coordination Private Insurance Innovation Center Regulations & Guidance Research, Statistics, Data & Systems Outreach & Education

Home > Hospital Price Transparency

Home Hospitals Consumers Resources Contact Us

 **Hospital Price Transparency**

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:

1. As a comprehensive machine-readable file with all items and services.
2. In a display of shoppable services in a consumer-friendly format.

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)

- 
- **Robo-Calling or**
 - **Using Pre-Recorded Voice**

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, whether “live” or prerecorded, 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.

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

TCPA: Limits on Healthcare Calls

- Effective 7/20/23:
 - For healthcare calls, must limit to no more than 1 call per day up to 3 calls per week;
 - For other calls, must limit number of robocalls to landline phone number to 3 during consecutive 30-day period;
 - Honor request to opt-out; and
 - Stricter requirements for obtaining consent.

(47 CFR 64.1200)

- FCC has issued proposed rule that would:
 - Strengthens consumers' rights to grant or revoke consent, and
 - Simplify opt-out process.

(88 FR 42034 (6/29/23))

TCPA Resources

[https://www.ftc.gov/business-guidance/
resources/complying-telemarketing-sales-rule](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?](#)

Antitrust



Antitrust Laws

- Sherman Act § 1
 - Prohibits agreement and conspiracy in restraint of trade.
 - Sherman Act § 1
 - Prohibits monopolies or attempted monopolies.
 - Clayton Act § 7
 - Prohibits mergers or acquisitions if effect would lessen competition or result in monopoly.
 - Federal Trade Comm'n Act
 - Prohibits unfair methods of competition and unfair or deceptive acts or practices.
 - State laws
 - Criminal penalties
 - \$1,000,000 to \$100,000,000 fine
 - Prison up to 10 years
 - Civil penalties
 - Action by state or federal govt
 - Treble (3x) damages
 - Injunctive relief, e.g., divestiture, restrictions, etc.
 - Attorneys' fees
 - Private lawsuit
 - Treble damages
 - Injunctive relief
 - Attorneys' fees
- *But see Local Govt Antitrust Act*

FTC / DOJ Guidelines Withdrawn



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement

[Home](#) / [News and Events](#) / [News](#) / [Press Releases](#)

For Release

Federal Trade Commission Withdraws Health Care Enforcement Policy Statements

Outdated statements no longer serve as useful guidance or reflect market realities



July 14, 2023



Anti-Discrimination Rules



Anti-Discrimination Laws

LAWS

- Civil Rights Act Title VI
- Americans with Disability Act
- Age Discrimination Act
- Rehabilitation Act § 504
 - HHS has proposed new rules.
(88 FR 63392 (9/14/23))
- Affordable Care Act § 1557
 - HHS has proposed new rules.
(87 FR 47824 (8/4/22))
- State discrimination laws

RISKS

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

Anti-Discrimination Laws

DISABILITIES

- Must provide reasonable accommodation to ensure effective communication.
 - **Auxiliary aids**
- 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.

Anti-Discrimination Laws: Recent OCR Enforcement

Date	Alleged Conduct	Resolution
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
5/15/23	<p>MCR Health failed to provide auxiliary aid to deaf wife who accompanied patient.</p> <ul style="list-style-type: none"> Should give “primary consideration” to request for aid from person with disability 	Policy and training
3/23/23 99	Dearborn OBGYN refused request for sign language interpreter , cancelled appointment and terminated her as patient	Policies, training \$7,500 in damages

Anti-Discrimination Law: Other Developments

- HHS issued report to increase language access for LEPs, including focus areas:
 - Internet access.
 - Telephone access.
 - Access to programs and activities.

<https://www.hhs.gov/about/news/2023/05/24/hhs-releases-report-increase-language-access-persons-with-limited-english-proficiency.html>
- DOJ proposes rule on Accessibility for Web and Mobile App Access re State and Local Govt Entities (88 FR 51948 (8/4/23))
 - Standards for web accessibility.
 - May portend standards for private businesses.
- HHS proposes rule prohibiting discrimination against LGBTQI+ in HHS funded grants, programs and services. (88 FR 44750 (9/11/23)).

OCR Disability Resources

<https://www.hhs.gov/civil-rights/for-individuals/special-topics/hospitals-effective-communication/disability-resources-effective-communication/index.html>

- Sample policies and procedures
- Charts
- Bulletins
- FAQs
- Links to other resources

The screenshot shows the HHS.gov Civil Rights page. The header includes the HHS.gov logo and the U.S. Department of Health & Human Services. Below the header is a search bar with the text "I'm looking for..." and a magnifying glass icon. To the right of the search bar is a link to the "A-Z Index". Below the search bar are four navigation buttons: "Information for Individuals", "Filing a Complaint", "Information for Providers", and "Newsroom". Below these buttons is a breadcrumb trail: "HHS > Civil Rights Home > For Individuals > Special Topics in Civil Rights > Effective Communication in Hospitals > Disability Resources for Effective Communication". Below the breadcrumb trail is a table of contents for the "Civil Rights for Individuals and Advocates" section, with links to "Race, Color, National Origin", "Disability", "Age Discrimination", "Sex Discrimination & Harassment", "Title IX", "Section 1557", "Hill-Burton", and "Section 1553". To the right of the table of contents is a section titled "Disability Resources for Effective Communication OCR Resources". This section contains two bullet points: "OCR signs effective communication Dear Colleague Letter with the Health Resources and Services Administration (08/30/2016)" and "OCR signs effective communication Dear Colleague Letter with the Puerto Rico Hospital Association. (06/09/2015)". Each bullet point has links to "Read the Bulletin", "Read the Letter - PDF", and "En Español - PDF". At the bottom of the page are links for "Text Resize", "Print", and "Share".

HHS.gov U.S. Department of Health & Human Services

Civil Rights

I'm looking for... A-Z Index

Information for Individuals Filing a Complaint Information for Providers Newsroom

HHS > Civil Rights Home > For Individuals > Special Topics in Civil Rights > Effective Communication in Hospitals > Disability Resources for Effective Communication

Civil Rights for Individuals and Advocates

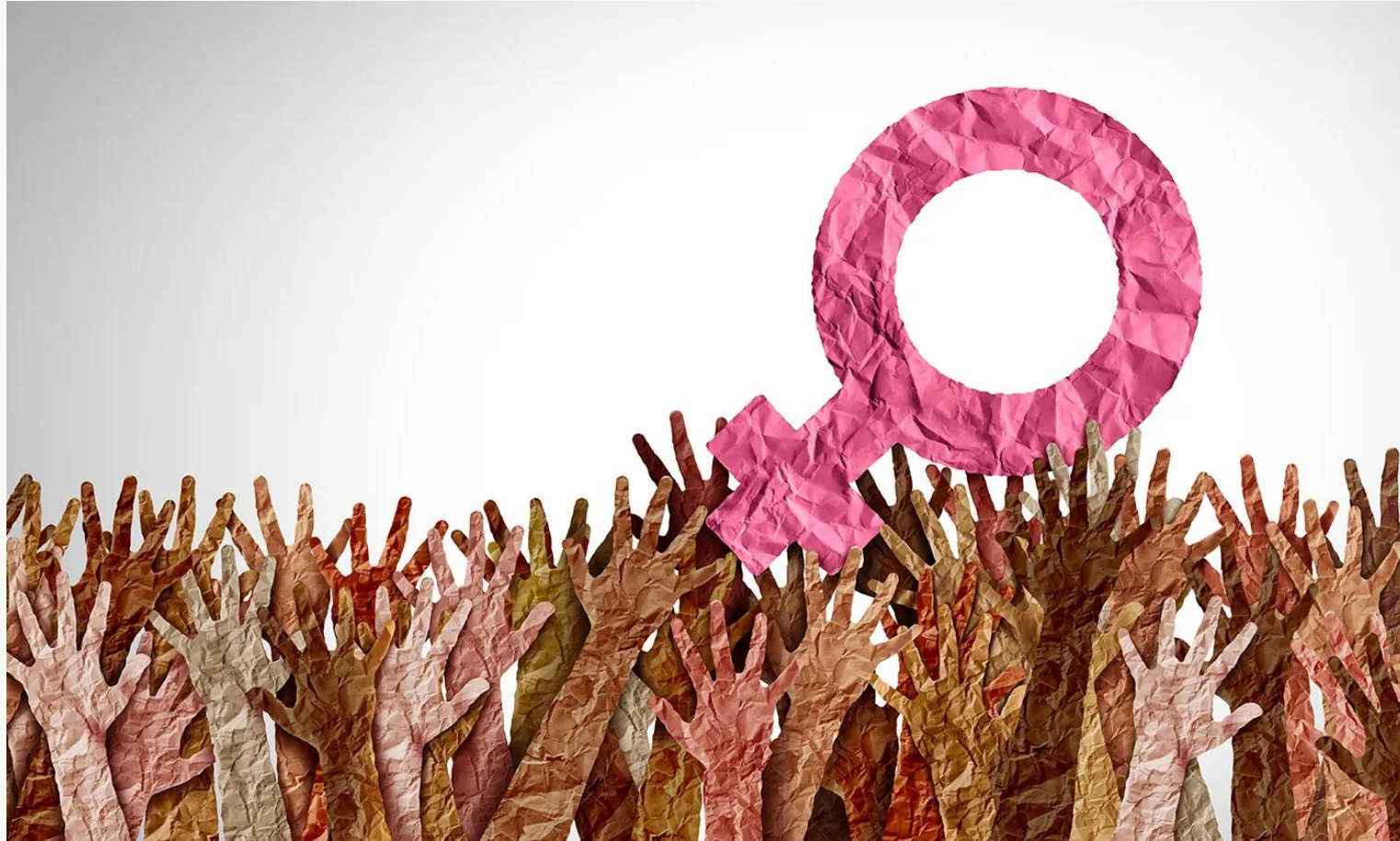
- Race, Color, National Origin
- Disability
- Age Discrimination
- Sex Discrimination & Harassment
- Title IX
- Section 1557
- Hill-Burton
- Section 1553

Text Resize A A A Print Share

Disability Resources for Effective Communication OCR Resources

- OCR signs effective communication Dear Colleague Letter with the Health Resources and Services Administration (08/30/2016)
 - [Read the Bulletin](#)
 - [Read the Letter - PDF](#)
 - [En Español - PDF](#)
- OCR signs effective communication Dear Colleague Letter with the Puerto Rico Hospital Association. (06/09/2015)

Reproductive Rights



ReproductiveRights.Gov

HHS has website concerning reproductive rights.

- Emergency care
 - EMTALA requires stabilizing treatment
- Birth control
 - ACA plans must cover birth control
- Medication
 - OCR guidance to pharmacies
- Access to abortion services
 - Depends on state law
- Other preventative health services
 - Insurance requirements

(<https://reproductiverights.gov/>)



REPRODUCTIVE RIGHTS.GOV

Know Your Rights:
Reproductive Health
Care

Reproductive Rights

- Availability of mifepristone for chemical abortions.
 - In 2000, FDA modified mifepristone subject to limitations.
 - In 2016, FDA updated regulations to extend mifepristone from 49 to 70 days of pregnancy and allowed APPs to prescribe.
 - In 2023, FDA modified rules to allow retail and online pharmacies to directly provide mifepristone via mail if prescribed in person or via telehealth.
 - In 4/23, Texas district court invalidated FDA's approval of mifepristone in 2000. (*Alliance for Hippocratic Medicine v. FDA* (N.D. Tex. 2023)). 5th Circuit upheld decision.
 - In 4/23, Supreme Court temporarily stayed district court order pending 5th Circuit appeal and writ of cert. (*Alliance for Hippocratic Medicine v. FDA* (S.Ct. 2023)).
 - In 8/23, 5th Circuit reversed district court's decision striking FDA's approval in 2000, but struck down FDA's 2016 and 2023 rules. (*Alliance for Hippocratic Medicine v. FDA* (5th Cir. 2023))
 - May not obtain mifepristone via mail or telehealth.
 - Limited to 49 days post-pregnancy.
 - DOJ intends to seek Supreme Court review.

Additional Resources



<https://www.hollandhart.com/healthcare>



People Capabilities

Search by keyword

Healthcare is a massive industry that needs specialized legal advice.

Healthcare spending represents about a fifth of US GDP. Few sectors are as complex and highly regulated. In an ultra-competitive environment, our industry-experienced team takes care of clients' legal issues so they can focus on business.

Our team handles a wide range of legal issues, including Stark, Anti-Kickback Statute, HIPAA, provider and payor contracting; mergers, acquisitions, and joint ventures; and medical staff issues; government investigations and compliance; employment; real estate; tax; employee benefits; and more. Because there is not much our healthcare clients face that we

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other



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

Primary Contacts



Kim Stanger

Partner

Boise
208.383.3913



Blaine Benard

Partner



Thank you!

Kim C. Stanger

Holland & Hart LLP

kcstanger@hollandhart.com

208-383-3913