

HEALTH INFO UPDATE: HIPAA, PART 2, AND INFO BLOCKING



KIM C. STANGER

(5-22)

DISCLAIMER

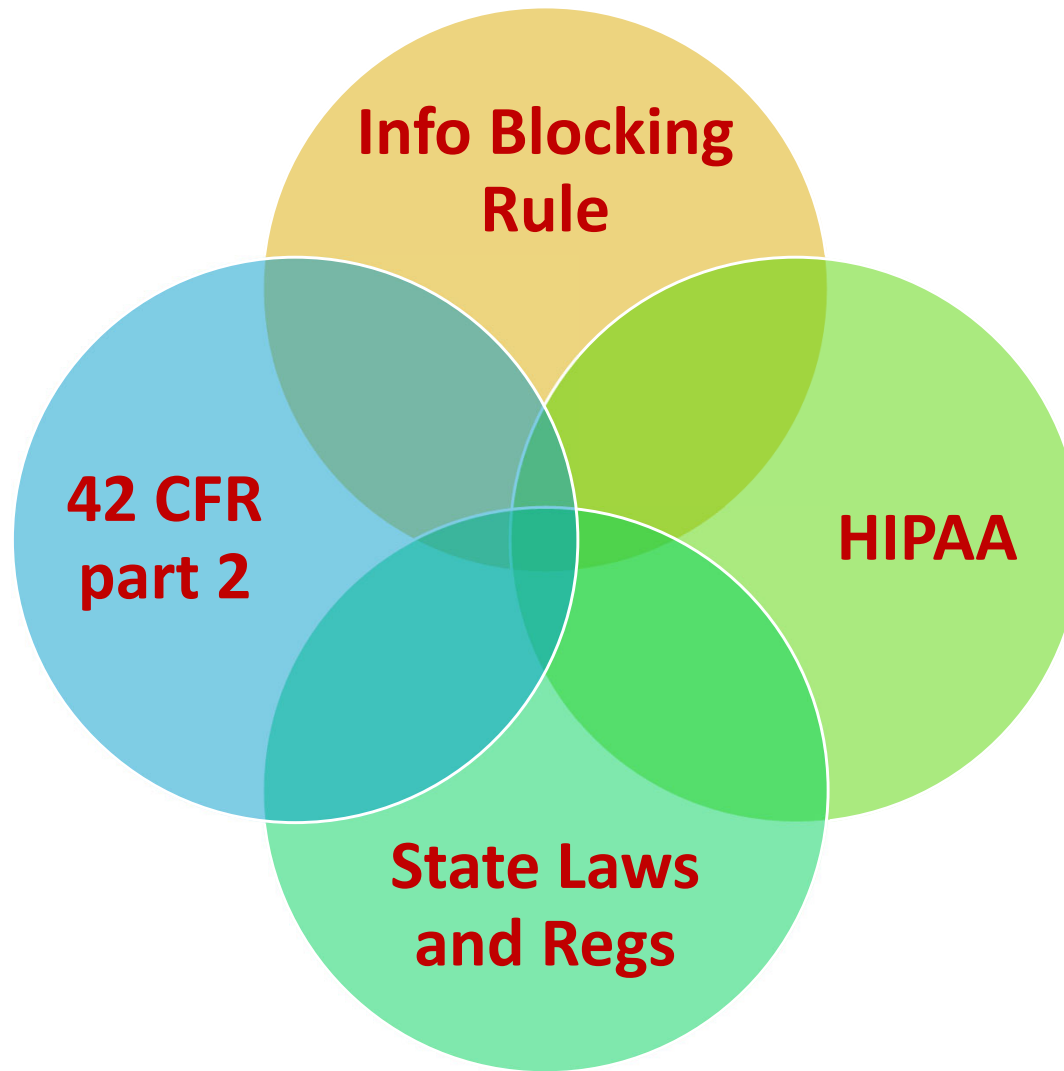
This presentation is designed to provide general information on pertinent legal topics. The information is provided for educational purposes only. Statements made or information included do not constitute legal or financial advice, nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author.

This information contained in this presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this presentation might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

PRELIMINARIES

- This is an overview.
 - Check relevant regulations when applying.
 - Application may depend on circumstances.
 - Consider other potentially applicable regs.
- We're going to be moving fast...
- Won't cover all slides, but decided to leave slides in as a resource for you.
- If you did not receive the slides, contact cphippen@hollandhart.com.
- If you have questions:
 - Submit them using chat feature, or
 - E-mail me at kcstanger@hollandhart.com.

LAWS OVERLAP AND MAY CONFLICT



COMPLY WITH MOST RESTRICTIVE LAW



42 CFR part 2

Info Blocking Rule

HIPAA

Other state or federal law

- Must generally comply with the most restrictive federal or state law, i.e.,
 - Law that gives greater protection to patient info, or
 - Law that gives greater control of their info to the patient.

HIPAA PRIVACY RULE, 45 CFR 164.500-.530



HIPAA CRIMINAL PENALTIES

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

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

HIPAA CIVIL PENALTIES

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)

HOLLAND & HART^{LLP}



ENFORCEMENT

- Must self-report breaches of unsecured protected health info
 - To affected individuals.
 - To HHS.
 - To media if breach involves > 500 persons.
- In future, individuals may recover % of penalties or settlement.
 - On 4/6/22, HHS issued request for information about issued notice soliciting input. (87 FR 19833)
- Must sanction employees who violate HIPAA.
- Possible lawsuits by affected individuals or others.
- State attorney general can bring lawsuit.
 - \$25,000 fine per violation + fees and costs

HIPAA: AVOIDING CIVIL PENALTIES

You can likely avoid HIPAA civil penalties if

- YOU:**
- Have required policies and safeguards in place.
 - Execute business associate agreements.
 - Train personnel and document training.
 - Respond immediately to mitigate and correct any violation.
 - Timely report breaches if required.

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



ENTITIES SUBJECT TO HIPAA

- Covered entities
 - Health care providers who engage in certain electronic transactions.
 - Consider hybrid entities.
 - Health plans, including employee group health plans if:
 - 50 or more participants; or
 - Administered by third party (e.g., TPA or insurer).
 - Health care clearinghouses.
- Business associates of covered entities
 - Entities with whom you share PHI to perform services on your behalf.

Is your
health
plan
compliant?



PROTECTED HEALTH INFO

- Protected health info (“PHI”) = info
 - Is created or received by a health care provider or health plan;
 - Relates to the past, present, or future physical or mental health; health care, or payment for health care to an individual; and
 - That either
 - Identifies the individual; or
 - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(45 CFR 160.103)

NOT COVERED BY HIPAA

- Info after person has been dead for 50 years.
- Info maintained in capacity other than as provider.
 - e.g., as employment records
- “De-identified” info, i.e., remove certain identifiable info
 - Names
 - Dates
 - Telephone, fax, and e-mail
 - Social Security Number
 - Medical Record Number
 - Account numbers
 - Biometric identifiers
 - Full face photos and comparable images
 - Other unique identifying number, characteristic, or code

(45 CFR 160.103, 164.514)

*Presume
PHI
protected
by HIPAA*

USE AND DISCLOSURE RULES (45 CFR 164.502-.514)



**Don't access
if don't need
to know.**

**Don't disclose
unless fit
exception or have
authorization**

**Implement
reasonable
safeguards**

TREATMENT, PAYMENT OR OPERATIONS

- May use/disclose PHI without patient's authorization for your own treatment, payment, or health care operations (as defined in rules).
- May disclose PHI to another covered entity for other covered entity's treatment, payment, or certain healthcare operations if both have relationship with patient.
- Exceptions: need patient authorization if--
 - Psychotherapy notes.
 - Agree with patient not to use or disclose for treatment, payment or healthcare operations.
 - *Don't agree to limit such use or disclosure!*

(45 CFR 164.506, 164.508 and 164.522)

PERSONS INVOLVED IN CARE

- May use or disclose PHI to family or others involved in patient's care or payment for care:
 - If patient present, may disclose if:
 - Patient agrees to disclosure or has chance to object and does not object, or
 - Reasonable to infer agreement from circumstances.
 - If patient unable to agree, may disclose if:
 - Patient has not objected; and
 - You determine it is in the best interest of patient.
 - Limit disclosure to scope of person's involvement.
- Applies to disclosures after the patient is deceased.

(45 CFR 164.510)

FACILITY DIRECTORY

- May disclose limited PHI for facility directory if:
 - Gave patient notice and patient does not object, and
 - Requestor asks for the person by name.
- If patient unable to agree or object, may use or disclose limited PHI for directory if:
 - Consistent with person's prior decisions, and
 - Determine that it is in patient's best interests
- Disclosure limited to:
 - Name
 - Location in facility
 - General condition
 - Religion, if disclosure to minister

(45 CFR 164.510)

EXCEPTIONS FOR PUBLIC HEALTH OR GOVERNMENT FUNCTIONS

- Another law requires disclosures
- Disclosures to prevent serious and imminent harm.
 - Proposed rule would make it easier to disclose.
- Public health activities
- Health oversight activities
- Judicial or administrative proceedings
 - Court order or warrant
 - Subpoenas
- Law enforcement
 - Must satisfy specific requirements
- Workers compensation

(45 CFR 164.512)

Ensure you
comply with
specific
regulatory
requirements

AUTHORIZATION

- Must obtain a valid written authorization to use or disclose protected PHI:
 - Psychotherapy notes.
 - Marketing
 - Sale of PHI
 - Research
 - For all other uses or disclosures unless a regulatory exception applies.
- Authorization may not be combined with other documents.
- Authorization must contain required elements and statements.

(45 CFR 164.508)

EMPLOYEE VACCINATIONS, TESTS, OR PHYSICALS; DRUG TESTS; IMES, ETC.

- HIPAA generally applies anytime you are rendering care as a healthcare provider, including:
 - Employee vaccinations or tests.
 - Employment physicals or drug screens.
 - Independent medical exams (“IMEs”).
 - School physicals.
 - Others?
- Must have patient’s authorization or HIPAA exception to use or disclose info, including use or disclosure for employment-related purposes.

(65 FR 82592 and 82640; 67 FR 53191-92)

➤ *Suggestions*

- *Obtain authorization before providing service.*
- *Provider may condition exam on authorization.*
- *Employer may condition employment on authorization.*

MARKETING

- Generally need authorization for “marketing”, i.e., communication about a product or service that encourages recipient to purchase or use product or service except:

Not defined as
“Marketing”

- To describe product or service provided by the covered entity,
- For treatment or healthcare operations, or
- For case management, care coordination, or to direct or recommend alternative treatment, therapies, providers, or setting,

unless covered entity receives financial remuneration from third party for making the communication.

(45 CFR 164.501 and .508(a)(3))

PERSONAL REPRESENTATIVES

- Under HIPAA, treat the personal rep as if they were the patient.
- Personal rep may exercise patient rights.
- Personal rep = persons with authority under state law to:
 - Make healthcare decisions for patient, or
 - Make decisions for deceased patient's estate.
- For example, in Idaho, personal reps =
 - Court appointed guardian
 - Agent in DPOA
 - Spouse
 - Adult child
 - Parent
 - Delegation of parental authority
 - Other appropriate relative
 - Any other person responsible for patient's care

(IC 39-4504)

➤ Check your state law!

PERSONAL REPRESENTATIVES

- Not required to treat personal rep as patient (i.e., not required to disclose PHI to them) if:
 - Minor has authority to consent to care.
 - Minor obtains care at the direction of a court or person appointed by the court.
 - Parent agrees that provider may have a confidential relationship.
 - Provider determines that treating personal representative as the patient is not in the best interest of patient, e.g., abuse.

(45 CFR 164.502(g))

[HTTPS://WWW.HHS.GOV/SITES/DEFAULT/FILES/S/PROVIDER_FFG.PDF](https://www.hhs.gov/sites/default/files/provider_ffg.pdf)



A HEALTH CARE PROVIDER'S GUIDE TO THE HIPAA PRIVACY RULE:



Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care

U.S. Department of Health and Human Services • Office for Civil Rights

This guide explains when a health care provider is allowed to share a patient's health information with the patient's family members, friends, or others identified by the patient as involved in the patient's care under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA is a Federal law that sets national standards for how health plans, health care clearinghouses, and most health care providers are to protect the privacy of a patient's health information.¹

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care. This guide is intended to clarify these HIPAA requirements so that health care providers do not unnecessarily withhold a patient's health information from these persons. This guide includes common questions and a table that summarizes the relevant requirements.²

COMMON QUESTIONS ABOUT HIPAA

- 1. If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?**

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Here are some examples:

- An emergency room doctor may discuss a patient's treatment in front of the patient's friend if the patient asks that her friend come into the treatment room.

BUSINESS ASSOCIATES

- May disclose PHI to business associates if have valid business associate agreement (“BAA”).

(45 CFR 164.502)

- Failure to execute BAA = HIPAA violation
 - May subject you to HIPAA fines.
 - Recent settlement: gave records to storage company without BAA: \$31,000 penalty.
 - Based on OCR settlements, may expose you to liability for business associate’s misconduct.
 - Turned over x-rays to vendor; no BAA: \$750,000.
 - Theft of business associate’s laptop; no BAA: \$1,550,000.

BUSINESS ASSOCIATES

- Business associates =
 - Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.
 - Covered entities acting as business associates.
 - Subcontractors of business associates.

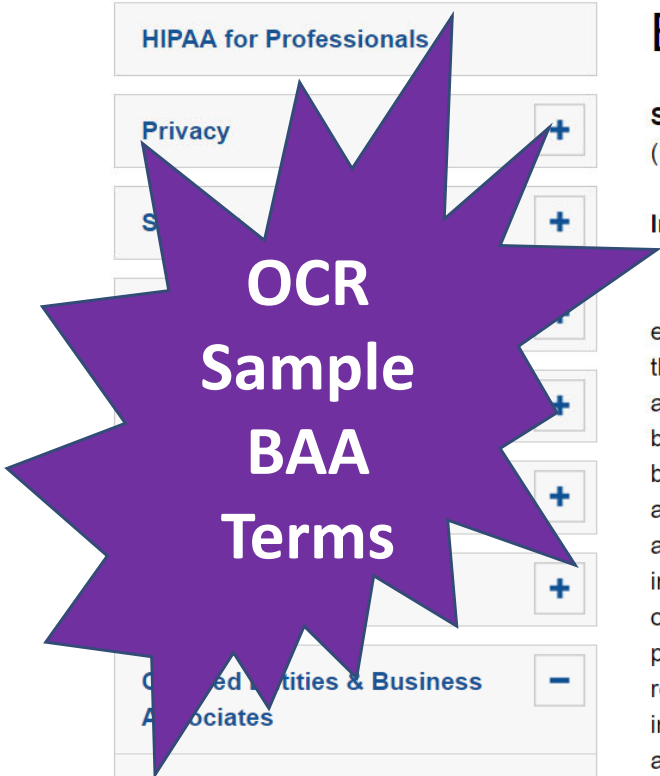
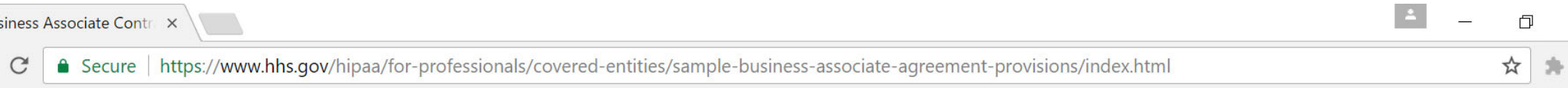
(45 CFR 160.103)

- BAAs must contain required terms and statements, e.g.,
 - Identify permissible uses
 - Pass limits to business associate and subcontractors

(45 CFR 164.314, 164.504(e))

➤ *Beware business associate's use of PHI for its own purposes.*

[HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/COVERED-ENTITIES/SAMPLE-BUSINESS-ASSOCIATE-AGREEMENT-PROVISIONS/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html)



- HIPAA for Professionals
- Privacy +
- S +
- +
- +
- +
- +
- Covered Entities & Business Associates -
 - Business Associates
 - Business Associate Contracts
- Training & Resources

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS (Published January 25, 2013)

Introduction

A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A “business associate” also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to

VERIFICATION

- Before disclosing PHI:
 - Verify the identity and authority of person requesting info if he/she is not known.
 - *E.g., ask for SSN or birthdate of patient, badge, credentials, etc.*
 - Obtain any documents, representations, or statements required to make disclosure.
 - *E.g., written satisfactory assurances for subpoena, representations from police that they need info for immediate identification purposes, etc.*

(45 CFR 164.514(f))

- Portals should include appropriate access controls.

(OCR Guidance on Patient's Right to Access Their Information)

MINIMUM NECESSARY STANDARD

- Cannot use or disclose more PHI than is reasonably necessary for intended purpose.
- Minimum necessary standard does not apply to disclosures to:
 - Patient.
 - Provider for treatment.
 - Per individual's authorization.
 - As required by law.
- Must adopt minimum necessary policies.
 - Identify those who have need to know.
 - Routine requests and routine disclosures.

(45 CFR 164.502 and .514)

PATIENT RIGHTS

- Notice of Privacy Practices
 - *Proposed rule would modify requirements to obtain acknowledgement of receipt.*
- Request restrictions on use or disclosure.
 - *Don't agree to restrictions.*
- Receive communications by alternative means.
- **Access to info.**
 - *OCR targeting access issues.*
 - *Consider effects of Info Blocking Rule.*
- Amendment of info.
- Accounting of disclosures of info.

(45 CFR 164.520 et. seq.)

PATIENT REQUESTS TO SEND PHI TO THIRD PARTY

On January 23, 2020, *Ciox* court modified OCR rules for disclosures per patient's request to send PHI to third party.

ePHI IN EHR	OTHER PHI
Must send ePHI maintained in EHR to third party identified by patient.	<u>Not</u> required to send to third party per patient's request.
Part of patient's right to access, i.e., must respond within 30 days.	N/A
<u>Not</u> limited to reasonable cost-based fee ("patient rate")	<u>Not</u> limited to reasonable cost-based fee ("patient rate")

(45 CFR 164.524; OCR *Guide to Patient Access*)

[WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/PRIVACY/GUIDANCE/ACCESS/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)

Individuals' Right under

Secure | <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/>

HHS.gov
Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...



[HHS A-Z Index](#)



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance](#) > Individuals' Right under HIPAA to Access their Health Information

Text Resize **A A A**

Print

Share



**Required
Reading!**

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

[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

ADMINISTRATIVE REQUIREMENTS

- Designate HIPAA privacy and security officers.
- Implement policies and safeguards.
- Train workforce and document training.
- Respond to complaints.
- Mitigate violations.
- Maintain documents required by HIPAA for 6 years.
 - *E.g., NPP, authorizations, designations, notices, etc.*
 - *Not medical records.*

(45 CFR 164.530)

HIPAA: PROPOSED RULES

- On 1/21/21, HHS proposed significant changes to HIPAA.
 - 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 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 (“NPP”).
 - Modifies content of NPP.

(86 FR 6446)

➤ *No final rule yet.*

HIPAA SECURITY RULE, 45 CFR 164.300-.318



HIPAA SECURITY RULE

- Risk assessment
- Implement safeguards.
 - Administrative
 - Technical, including encryption
 - Physical
- Execute business associate agreements.

(45 CFR 164.300 et seq.)

Protect ePHI:

- Confidentiality
- Integrity
- Availability



[HTTPS://WWW.HEALTHIT.GOV/TOPIC/PRIVACY-SECURITY-AND-HIPAA/SECURITY-RISK-ASSESSMENT-TOOL](https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool)

Security Risk Assessment Tool | H x +

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

NEW: Health IT Feedback Portal CONTACT EMAIL UPDATES

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

Connect with us: in t y r

TOPICS | BLOG | NEWS | DATA | ABOUT ONC

Search

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA

Educational Videos

- Security Risk Assessment Tool**
- Security Risk Assessment Videos
- Top 10 Myths of Security Risk Analysis

HIPAA Basics

Privacy & Security Resources & Tools

Model Privacy Notice (MPN)

How APIs in Health Care can Support Access to Health Information: Learning Module

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA Security Rule technical safeguards. A risk assessment also helps reveal areas where your organization's health information (PHI) could be at risk. To learn more about the assessment process and the benefits your organization, visit the [Office for Civil Rights' official guidance](#).

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in partnership with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment Tool to help guide you through the process. The tool is designed to help healthcare organizations conduct a security risk assessment as required by the HIPAA Security Rule. The tool is available for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) systems.

[Download Version 3.2 of the SRA Tool \[.msi - 94 MB\]](#)

All information entered into the SRA Tool is stored locally to the users' computer or device. HHS does not receive, collect, view, store or transmit any information entered in the SRA Tool. The results of the assessment are displayed in a report which can be used to determine risks in policies, processes

[Submit Questions Or Feedback](#)

SRA Webinars

[HTTPS://WWW.HEALTHIT.GOV/TOPIC/PRIVACY-SECURITY-AND-HIPAA/HEALTH-IT-PRIVACY-AND-SECURITY-RESOURCES-PROVIDERS](https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers)



- Privacy, Security, and HIPAA
- Educational Videos
- Security Risk Assessment Tool
- HIPAA Basics
- Privacy & Security Resources & Tools
- Resources and Tools for Consumers
- Resources and Tools for Providers
- Security Risk Assessment Tool
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module

Health IT Privacy and Security Resources for Providers

The Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and other HHS agencies have developed a number of resources for you. These resources, guides, and toolkits are intended to help you better integrate HIPAA and other federal health information privacy requirements into your business processes.

Tools and Templates

- Sync for Science (S4S) API Privacy and Security [PDF - 939 KB]. Led a privacy and security analysis, and assessment of a voluntary subset of S4S pilot organizations.
- Guide to Privacy and Security of Electronic Health Information. This guide helps providers succeed in their privacy and security responsibilities. The Guide covers the privacy and security management process.
- Security Risk Assessment (SRA) Tool. HHS downloadable tool to help providers conduct the risk analysis process.
- Security Risk Analysis Guidance. OCR's expectations for how providers can meet the risk analysis requirements of the HIPAA Security Rule.
- HIPAA Security Toolkit Application. National Institute of Standards and Technology (NIST) toolkit to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.



WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SECURITY/GUIDANCE/INDEX.HTML

The Security Rule | HHS.gov

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



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > The Security Rule

HIPAA for Professionals

Regulatory Initiatives

Privacy



Security



Summary of the Security Rule

Security Guidance

Cyber Security Guidance

Breach Notification



Compliance & Enforcement



Text Resize **AAA**

Print

Share

The Security Rule

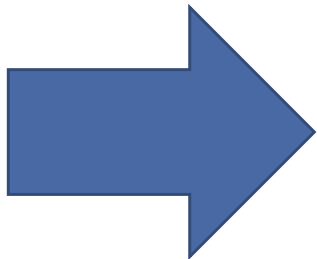
The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The Security Rule is located at 45 CFR [Part 160](#) and Subparts A and C of [Part 164](#).

[View the combined regulation text](#) of all HIPAA Administrative Simplification Regulations found at 45 CFR 160, 162, and 164.

Security Rule History

January 25, 2013 – [Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health \(HITECH\) Act and the Genetic Information Nondiscrimination Act, and Other Modifications – Final Rule - PDF](#) (The "Omnibus HIPAA Final Rule")



ENCRYPTION

- Encryption is an addressable standard per 45 CFR 164.312:
 - (e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.
 - (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
- ePHI that is properly encrypted is “secured”.
 - *Not subject to breach reporting.*
- OCR presumes that loss of unencrypted laptop, USB, mobile device is breach.
 - *But see HHS v. M.D. Anderson (5th Cir. 2021)*

[HTTPS://WWW.HEALTHIT.GOV/RESOURCE/YOUR-MOBILE-DEVICE-AND-HEALTH-INFORMATION-PRIVACY-AND-SECURITY](https://www.healthit.gov/resource/your-mobile-device-and-health-information-privacy-and-security)

Home

Topics

Blog

News

Data

About ONC

Your Mobile Device and Health Information Privacy and Security

Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.

**Beware
Mobile
Devices**

This guide was developed from the experiences of Regional Extension Center staff in the performance of technical support to primary care providers. The information contained in this guide is not intended to serve as legal advice nor should it be used as such. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information herein. The U.S. Government or the U.S. Department of Health and Human Services does not endorse or make any specific resources, tools, products, process, service, manufacturer, or company does not constitute its endorsement or approval of any specific resources, tools, products, process, service, manufacturer, or company.

Your Mobile Device and Health Information Privacy and Security

Audience

Providers & Professionals

Resource Topics

Privacy and Security

COMMUNICATING BY E-MAIL OR TEXT

- General rule: must be secure, i.e., encrypted.
- To patients: may communicate via unsecure e-mail or text if warned patient and they choose to receive unsecure.

(45 CFR 164.522(b); 78 FR 5634)

- To providers, staff or other third parties: must use secure platform.

(45 CFR 164.312; CMS letter dated 12/28/17)

- Orders: Medicare Conditions of Participation and Conditions for Coverage generally prohibit texting orders.

(CMS letter dated 12/28/17)

CYBERSECURITY: SECURITY RULE IN ACTION...



[HTTPS://WWW.HHS.GOV/BLOG/2022/02/28/IMPROVING-CYBERSECURITY-POSTURE-HEALTHCARE-2022.HTML](https://www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html)

I'm looking for...



[A-Z Index](#)

[Home](#) > [Blog](#) > [Improving the Cybersecurity Posture of Healthcare in 2022](#)

Categories

- [Coronavirus \(8\)](#)
- [Fraud \(1\)](#)
- [Global Health \(1\)](#)
- [Grants and Contracts \(1\)](#)
- [Health Data \(1\)](#)
- [Health IT \(3\)](#)
- [HIPAA \(1\)](#)
- [Holidays and Observances \(2\)](#)
- [Prevention and Wellness \(3\)](#)
- [Public Health and Safety \(4\)](#)
- [Research \(2\)](#)

44

Text Resize [A](#) [A](#) [A](#)

Print

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

Improving the Cybersecurity Posture of Healthcare in 2022

February 28, 2022 | By: [Lisa Pino](#), Director for Office for Civil Rights (OCR)

Summary: Encourages HIPAA covered entities and business associates to strengthen their cyber posture in 2022.



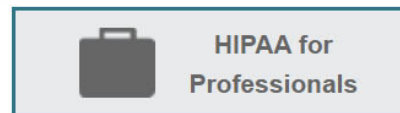
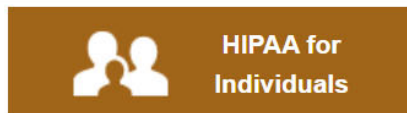
CYBERSECURITY

“I cannot underscore enough the importance of enterprise-wide risk analysis.... You should fully understand where all electronic protected health information (ePHI) exists across your organization – from software, to connected devices, legacy systems, and elsewhere across your network.... Some best practices include:

- “Maintaining offline, encrypted backups of data and regularly test your backups;
- “Conducting regular scans to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface;
- “Regular patches and updates of software and Operating Systems; and
- “Training your employees regarding phishing and other common IT attacks.”

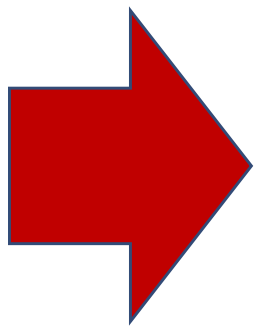
(Lisa Pino, Director of Office for Civil Rights (2/28/22))

[HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SECURITY/GUIDANCE/CYBERSECURITY-NEWSLETTER-FIRST-QUARTER-2022/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html)



[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [The Security Rule](#) > [Security Rule Guidance Material](#) > OCR Quarter 1 2022 Cybersecurity Newsletter

- HIPAA for Professionals
- Regulatory Initiatives
- Privacy +
- Security -
 - Summary of the Security Rule
 - Security Guidance
 - Cyber Security Guidance
- Breach Notification +
- Compliance & Enforcement +
- Special Topics +



Text Resize **A A A** | Print | Share

OCR Quarter 1 2022 Cybersecurity Newsletter

Defending Against Common Cyber-Attacks

Throughout 2020 and 2021, hackers have targeted the health care industry seeking unauthorized

Addresses:

- Phishing
- Exploiting known vulnerabilities
- Weak cybersecurity practices
- List of resources

preventative steps regulated entities can take to protect against some of the more common, and often successful, cyber-attacks.

HTTPS://WWW.CISA.GOV/STOPRANSOMWARE

Stop Ransomware | CISA

https://www.cisa.gov/stopransomware

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



Search



**WHAT IS
RANSOMWARE?**

[LEARN MORE](#)

**HAVE YOU
BEEN HIT BY
RANSOMWARE?**

[LEARN MORE](#)

Known Exploited
Vulnerabilities
Catalog

cisa.gov

UPdated



Locum Tenens Billi...pdf

Show all



[HTTPS://WWW.PHE.GOV/PREPAREDNESS/PLANNING/405D/DOCUMENTS/HICP-MAIN-508.PDF](https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf)

Recommended Practices

1. E-mail protection system
2. Endpoint protection system
3. Access management
4. Data protection and loss prevention
5. Network management
6. Vulnerability management
7. Incident response
8. Medical device security
9. Cybersecurity policies

- Sample Forms
- Resources

/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients



[HTTPS://WWW.HHS.GOV/ABOUT/AGENCIES/ASA/OCIO/HC3/INDEX.HTML](https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html)

agencies/asa/ocio/hc3/index.html



Search...



Tools ?

[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](#)

Text Resize **A A A**

Print

Share



Health Sector Cybersecurity Coordination Center (HC3)

A Prescription for Health Sector Cybersecurity

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



HC3 Products

Threat Briefs

Highlights relevant cybersecurity topics and raises the HPH sector's situational

Sector Alerts

Provides high-level, situational background information and context for technical and

HIPAA BREACH NOTIFICATION RULE, 45 CFR 164.400-.420



BREACH NOTIFICATION

- If there is “breach” of “unsecured PHI”,
 - Covered entity must notify:
 - Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed.
 - HHS.
 - Local media, if breach involves > 500 persons in a state.
 - Business associate must notify covered entity.

(45 CFR 164.400 et seq.)

“BREACH” OF UNSECURED PHI

- Acquisition, access, use or disclosure of PHI in violation of privacy rule is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors:
 - nature and extent of PHI involved;
 - unauthorized person who used or received the PHI;
 - whether PHI was actually acquired or viewed; and
 - extent to which the risk to the PHI has been mitigated,unless an exception applies.

(45 CFR 164.402)

NOT A “BREACH” OF UNSECURED PHI

- Loss of “secured” data, e.g., properly encrypted.
- Incidental disclosure, i.e., disclosure that is incidental to permissible disclosure so long as covered entity implemented reasonable safeguards. (45 CFR 164.502(a)(1)(iii))
- “Breach” defined to exclude:
 - Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of privacy rule.
 - Inadvertent disclosure by authorized person to another authorized person at same covered entity, and PHI not further used or disclosed in violation of privacy rule.
 - Disclosure of PHI where covered entity has good faith belief that unauthorized person receiving info would not reasonably be able to retain info.

(45 CFR 164.402)

NOTICE TO INDIVIDUAL

- Without unreasonable delay but no more than 60 days of discovery.
 - When known by anyone other than person who committed breach.
- Written notice to individual.
 - By mail.
 - Must contain elements, including:
 - Description of breach
 - Actions taken in response
 - Suggested action individual should take to protect themselves.

(45 CFR 164.404(d))

NOTICE TO HHS

- If breach involves fewer than 500 persons:
 - Submit to HHS annually within 60 days after end of calendar year in which breach was discovered (i.e., by March 1).
- If breach involves 500 or more persons:
 - Notify HHS contemporaneously with notice to individual or next of kin, i.e., without unreasonable delay but within 60 days.

(45 CFR 164.408)

- Submit report at <http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>.

[HTTPS://WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/BREACH-NOTIFICATION/BREACH-REPORTING/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html)

Chief Reporting | HHS x

www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

The Church of J... Mormon Channel Idaho Statutes Google Accounts Stake/Ward Lea... Outlook.com - ... Stewardship Ma... AHLA The American H... AHLA listsere Pandora Int

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services



HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

HIPAA for Professionals

Privacy



Security



Breach Notification



Breach Reporting

Guidance

Reports to Congress

Regulation History

Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business Associates

Training & Resources

Text Resize A A A

Print

Share



Submitting Notice of a Breach to the Secretary

A covered entity must notify the Secretary if it discovers a breach of unsecured protected health information. See [45 C.F.R. § 164.408](#). All notifications must be submitted to the Secretary using the Web portal below.

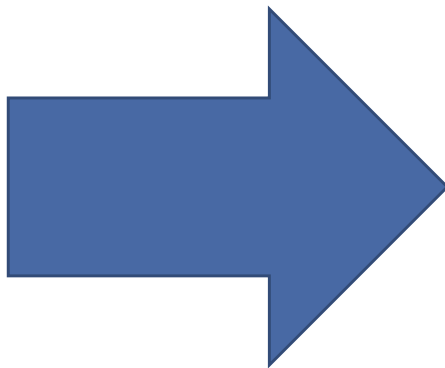
A covered entity's breach notification obligations differ based on whether the breach affects 500 or more individuals or fewer than 500 individuals. If the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate, and, if it discovers additional information, submit updates in the manner specified below. If only one option is available in a particular submission category, the covered entity should pick the best option, and may provide additional details in the free text portion of the submission.

If a covered entity discovers additional information that supplements, modifies, or clarifies a previously submitted notice to the Secretary, it may submit an additional form by checking the appropriate box to indicate that it is an addendum to the initial report, using the transaction number provided after its submission of the initial breach report.

Please review the instructions below for submitting breach notifications.

Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.



HHS "WALL OF SHAME"

- HHS posts list of those with breaches involving more than 500 at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsfpersons

The screenshot shows a web browser window with the URL https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. The page header includes the text "U.S. Department of Health and Human Services Office for Civil Rights" and "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". Below the header is a navigation bar with three buttons: "Under Investigation", "Archive", and "Help for Consumers".

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

[Show Advanced Options](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
0	Julieta Y. Echeverria D.D.S., Inc.	CA	Healthcare Provider	529	05/20/2022	Theft	Paper/Films

NOTICE TO MEDIA

- If breach involves unsecured PHI of more than 500 residents in a state, covered entity must notify prominent media outlets serving that state (e.g., issue press release).
 - Without unreasonable delay but no more than 60 days from discovery of breach.
 - Include same content as notice to individual.

(45 CFR 164.406)

➤ *Don't include PHI in your notice to media!*

NOTICE BY BUSINESS ASSOCIATE

- Business associate must notify covered entity of breach of unsecured PHI:
 - Without unreasonable delay but no more than 60 days from discovery.
 - Notice shall include to extent possible:
 - Identification of individuals affected, and
 - Other info to enable covered entity to provide required notice to individual.

(45 CFR 164.410)

➤ *Ensure BAA requires prompt notice of breach, e.g., within 5 business days.*

STATE BREACH REPORTING STATUTES



For example:

- Statute requires commercial entities to immediately investigate and notify subject persons if there is a
 - Breach of computer system
 - Resulting in illegal acquisition
 - Of certain unencrypted computerized personal info
 - Name + certain other identifiers (e.g., SSN, driver's license, credit card number + PIN or password, etc.)
 - Actual or reasonably likely misuse of personal info
- \$25,000 fine if fail to notify persons.
- Compliance with HIPAA may satisfy Idaho statute.

(IC 28-51-104)

INFORMATION BLOCKING RULE, 45 CFR 171



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 ONC
 - <https://www.healthit.gov/topic/information-blocking>.
- ONC investigations
- Proposed rule:
 - Civil monetary penalties of up to \$1,000,000 per violation

(85 FR 22979 (4/24/2020);
proposed 42 CFR 1003.1420)

Healthcare Providers

- “Appropriate disincentives to be established by HHS.”
- Waiting for rule.



INFO BLOCKING: EXAMPLES

- 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, e.g., patient consent.
- Action is reasonable under the circumstances.
- Action fits within regulatory exception.

INFO BLOCKING EXCEPTIONS



**PREVENTING
HARM
EXCEPTION**



**PRIVACY
EXCEPTION**



**SECURITY
EXCEPTION**

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



**INFEASIBILITY
EXCEPTION**



**HEALTH IT
PERFORMANCE
EXCEPTION**

8

**EXCEPTIONS TO THE
INFORMATION
BLOCKING
PROVISION**



**LICENSING
EXCEPTION**



**FEEES
EXCEPTION**



**CONTENT AND
MANNER
EXCEPTION**

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

HTTPS://WWW.HEALTHIT.GOV/TOPIC/INFORMATION-BLOCKING



HealthIT.gov | Official Website of The Office of the National Coordinator for Health Information Technology (ONC) | NEW: Health IT Feedback Portal | CONTACT | EMAIL UPDATES

Connect with us: [in](#) [tw](#) [yt](#) [rs](#)

TOPICS | BLOG | NEWS | DATA | ABOUT ONC

Search

HealthIT.gov > Topics > Information Blocking

- Information Blocking
- Report Information Blocking

Information Blocking

What is information blocking?

In general, information blocking is a practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that, except as required by law or specified by the Secretary of Health and Human Services (HHS) as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI).



Have questions about information blocking? [View our Information Blocking Frequently Asked Questions \(FAQs\)](#)

What are examples of practices that could constitute information blocking?

Section 4004 of the Cures Act specifies certain practices that could constitute information blocking:

- Practices that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law.

Additional Resources

- Fact Sheets
- Webinars
- FAQs
- [Report Information Blocking](#)

TIME FOR RESPONDING TO PATIENT REQUESTS

“Q: Are actors (for example, health care providers) expected to release test results to patients through a patient portal or application programming interface (API) as soon as the results are available to the ordering clinician?”

“While the [IBR] do[es] not require actors to proactively make electronic health information (EHI) available, once a request to access, exchange or use EHI is made actors must timely respond to the request (for example, from a patient for their test results). Delays or other unnecessary impediments could implicate the information blocking provisions.

“In practice, this could mean a patient would be able to access EHI such as test results in parallel to the availability of the test results to the ordering clinician.”

(<https://www.healthit.gov/curesrule/resources/information-blocking-faqs>).

TIME FOR RESPONDING TO PATIENT REQUESTS

“Q: When would a delay in fulfilling a request for access [to] EHI be considered an interference under the [IBR]?”

“A determination as to whether a delay would be an interference ... would require a fact-based, case-by-case assessment of the circumstances....”

“Likely to be an Interference: ... if a health care provider established [a] policy that ... imposed delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results.... [I]t also would likely be considered an interference

- where a delay in providing access ... occurs after a patient logs in to a patient portal to access EHI that a health care provider has (including, for example, lab results) and such EHI is not available—for any period of time—through the portal.
- where a delay occurs in providing a patient’s EHI via an API to an app that the patient has authorized to receive their EHI.”

(<https://www.healthit.gov/curesrule/resources/information-blocking-faqs>).

TIME FOR RESPONDING TO PATIENT REQUESTS

- **“Q: When a state or federal law or regulation, such as the HIPAA Privacy Rule, requires EHI be released by no later than a certain date after a request is made, is it safe to assume that any practices that result in the requested EHI’s release within that other required timeframe will never be considered information blocking?”**
- No. The information blocking regulations ... have their own standalone provisions....

(<https://www.healthit.gov/curesrule/resources/information-blocking-faqs>)

INFO BLOCKING RULE AND HIPAA

If HIPAA allows access or disclosure:

- IBR prohibits info blocking.
- IBR may require provider to allow access or disclosure even if HIPAA does not require it, e.g.,
 - Treatment, payment, operations.
 - Authorization.
- IBR may require quicker response than HIPAA.
 - > 30 days.

If HIPAA or other law prohibits disclosure:

- Not info blocking if conditions for access or disclosure are not satisfied, e.g.,
 - Patient consent.
 - Patient authorization.
 - Confirmation that HIPAA exception allows disclosure.

42 CFR PART 2

SUBSTANCE USE DISORDER RECORDS



SUBSTANCE USE DISORDER RECORDS

- 42 USC 290dd
- CARES Act 3221
- Confidentiality of Substance Use Disorder Patient Records, 42 CFR part 2
- HIPAA privacy and security regulations, 45 CFR part 164
- Other federal and state laws, e.g.
 - Information Blocking Rule
 - State laws re access or disclosure of SUD records

CONFIDENTIALITY OF SUBSTANCE USE DISORDER PATIENT RECORDS, 42 CFR PART 2

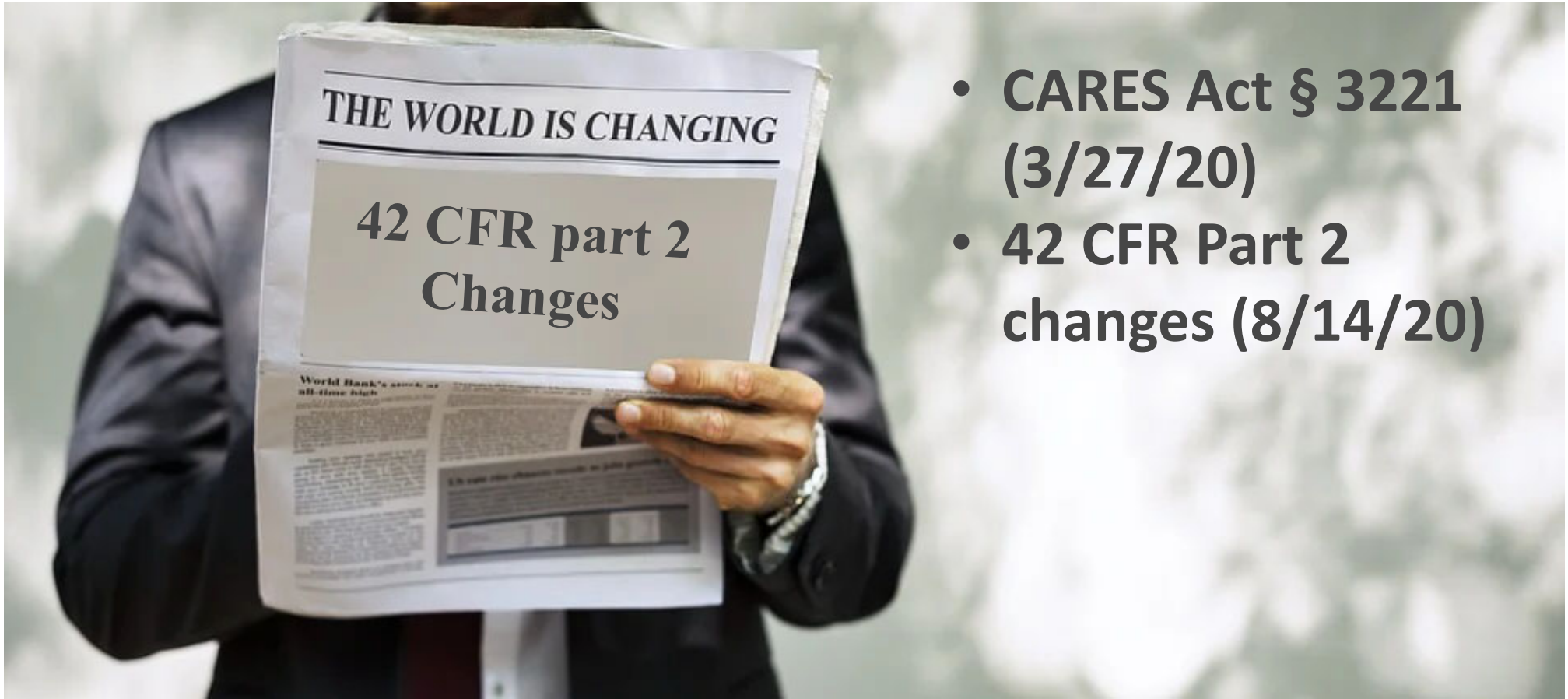
Purpose

- To encourage persons to obtain treatment for a substance use disorder (“SUD”) by limiting disclosure of info relating to their treatment.

Requirements

- In general, part 2 programs may not disclose any info that would identify a person as having, or having had, or being referred to a substance use disorder unless the person provides written consent or an exception applies.
- Certain entities to whom program discloses info must comply with part 2.

42 CFR PART 2 UPDATE



- CARES Act § 3221 (3/27/20)
- 42 CFR Part 2 changes (8/14/20)

CARES ACT § 3221

- Allows disclosure of SUD info for treatment, payment or healthcare operations if obtain initial consent.
- Replaces criminal penalties with HIPAA penalties.
- Requires breach notification for improper disclosure of SUD info.
- Requires HHS to update HIPAA notice of privacy practices rules.
- May share de-identified SUD info with public health authority
- Limits use of SUD info in criminal, civil and administrative proceedings.
- Prohibits discrimination based on SUD info.
- Requires HHS to promulgate regulations.

(CARES Act 3221, amending 42 USC 290dd)

REVISED 42 CFR PART 2 REGS (EFFECTIVE 8/14/20)

- *SAMHSA has not issued regs to implement Cares Act CARES Act § 3221.*
- SAMSHA did issue regs to implement rules proposed in 2019 to facilitate coordinated care.
 - Limits application to non-part 2 providers who record oral info or segregate part 2 records.
 - Consent requirements relaxed.
 - Easier to disclose to central registries and prescription drug monitoring programs.
 - Exception for medical emergencies expanded.
 - Modifies rules for research disclosures.
 - Modifies rules for audit disclosures.

(85 FR 42986 (7/15/20))

APPLICABILITY: 42 CFR PART 2

- Generally prohibits use or disclosure of records without patient consent if:
 - Record identifies a patient as having, having had, or referred for a substance use disorder (“SUD”); and
 - SUD record is created, obtained, or maintained by a federally assisted drug or alcohol abuse program.

(42 CFR 2.12(a))

- “SUD” = cluster of cognitive, behavioral and physiological symptoms indicating that the patient continues using substance despite significant substance-related problems such as impaired control, social impairment, risky use, tolerance and withdrawal.

(42 CFR 2.11)

APPLICABILITY: “FEDERALLY ASSISTED” PROGRAM

- “Federally assisted” =
 - Carried out under license or authorization granted by U.S. department or agency (e.g., participating in Medicare, DEA registration, etc.);
 - Supported by funds provided by a U.S. department or agency (e.g., receiving federal financial assistance, Medicaid, grants, etc.);
 - Program is tax-exempt or claims tax deductions relating to program; or
 - Conducted directly or by contract or otherwise by any dept or agency of the United States (but see rules re VA or armed forces).

(42 CFR 2.12(b))

- Not purely private pay programs.
 - *But HIPAA may still apply.*

APPLICABILITY: FEDERALLY ASSISTED “PROGRAM”

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

(42 CFR 2.11; 2.12(e))

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

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



APPLICABILITY: FEDERALLY ASSISTED "PROGRAM"

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

APPLICABILITY: FEDERALLY ASSISTED “PROGRAM”

- “Hold self out” = activity that would lead one to reasonably conclude that the individual or entity provides SUD diagnosis, treatment, or referral for treatment, e.g., through advertising or marketing.

(42 CFR 2.11; 2.12(e))

- May include state licensing procedures, advertising or posting notices, certifications in addiction medicine, listings in registries, internet statements, consultation activities for non-“program” practitioners, info presented to patients or families, etc.

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

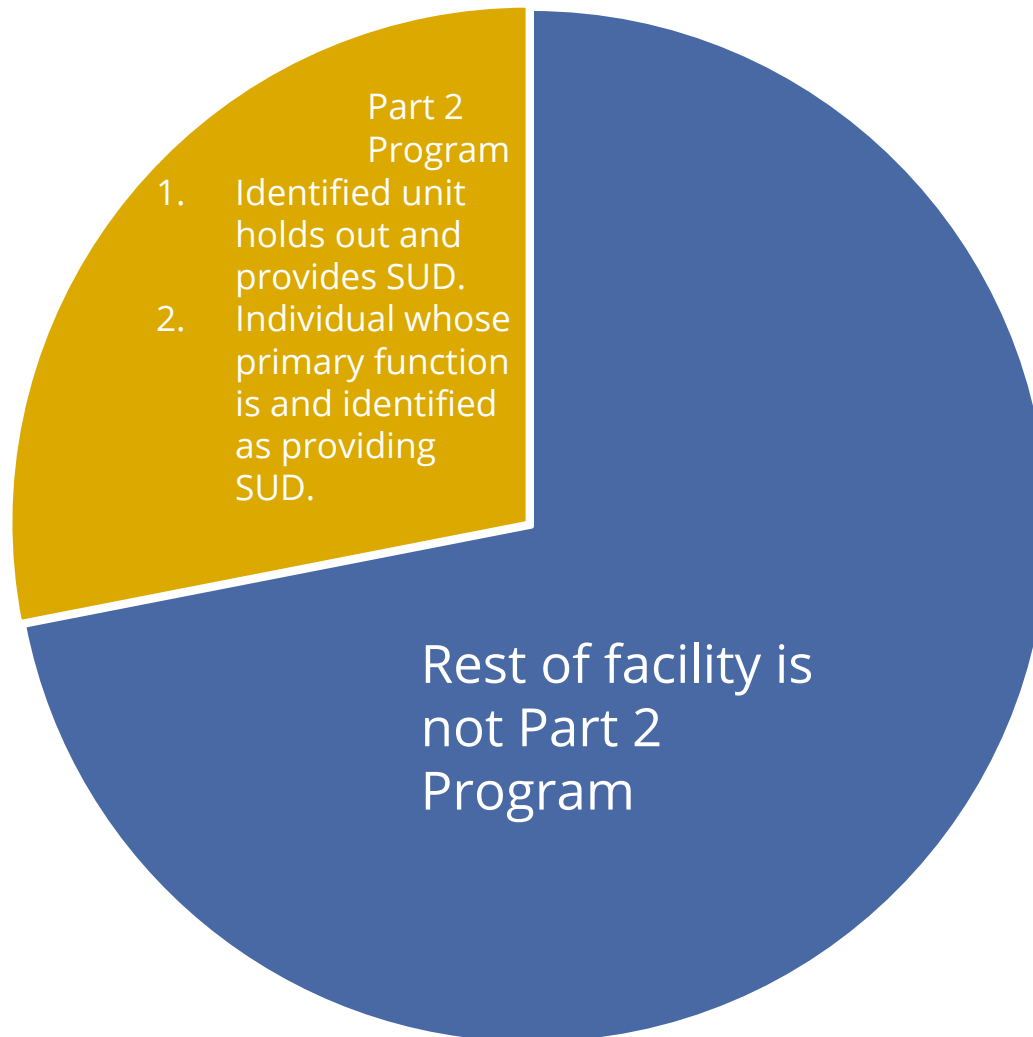
APPLICABILITY: FEDERALLY ASSISTED “PROGRAM”

- Part 2 program is not:
 - Emergency room personnel who treat overdose.
 - Providers who prescribe controlled substances to treat SUD but who do not hold themselves out as providing SUD treatment.

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

APPLICABILITY: FEDERALLY ASSISTED PROGRAM

General Medical Facility



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

ENTITIES THAT MUST MAINTAIN CONFIDENTIALITY

- Prohibition against disclosure applies to:
 - Part 2 program.
 - Entities having direct administrative control over the part 2 program.
 - “Lawful holders”, e.g., persons who appropriately:
 - Receive SUD info from a part 2 program, and
 - Receive required notice prohibiting redisclosure.

(42 CFR 2.12(d)(2), as amended)

DISCLOSURE OF SUD INFO

With patient's written consent

- For treatment, payment or healthcare operations.
- For other purposes specified in consent.
- Consent must contain required elements.
- Must include notice prohibiting redisclosure.

(CARES Act 3221; 42 CFR 2.31-2.33)

➤ *Compare HIPAA.*

Without patient's written consent

- Within part 2 program if need to know.
- To those with administrative control over program.
- Qualified Service Organization ("QSO") if have QSOA agreement ("QSOA")
- Medical emergency.
- Report to law enforcement if crime on premises or threat against program personnel.
- Report child abuse.
- Research subject to conditions.
- Audits and investigations subject to conditions.
- Per compliant order + subpoena.

NOTICE OF REDISCLOSURE

- If disclose with written consent, must include one of these notices with the SUD records produced:
 - “This record which has been disclosed to you is protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this record unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or, is otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§2.12(c)(5) and 2.65.”
- or
- “42 CFR part 2 prohibits unauthorized disclosure of these records.”

(42 CFR 2.32, as amended)

LIMITS ON DISCLOSURE

- Any disclosure of SUD records must be limited to that info which is necessary to carry out the purpose of the disclosure.

(42 CFR 2.13(a))

- *Similar to HIPAA “minimum necessary” standard.*

LAWFUL HOLDERS AND AGREEMENTS

- If patient gives written consent to disclosures for payment or healthcare operations, recipient (“lawful holder”) may further disclose to contractors, subs and legal representatives to carry out such purposes if:
 - Have written contract or other legal instrument by which contractor is bound by part 2.
 - Furnish notice of redisclosure.
 - Require recipient to implement appropriate safeguards to protect info.
 - Require recipient to report unauthorized uses, disclosures, or breaches.
 - Lawful holder discloses only minimum necessary.
 - Recipient may only further disclose to contracted entity to help them fulfill purposes of disclosure by lawful holder.

(42 CFR 2.33(b)-(c))

LAWFUL HOLDERS: DISCLOSURE FOR PAYMENT OR OPERATIONS

- Billing, claims, collections, etc.
- Clinical professional support, e.g., QA, utilization review, etc.)
- Patient safety activities
- Peer review, training, assessments, etc.
- Accreditation, certification, licensing, credentialing, etc.
- Underwriting, enrollment, premium rating, etc.
- Third party liability coverage.
- Address fraud, waste, abuse.
- Medical review, legal, auditing.
- Business planning, development
- Business management and general administrative duties.
- Customer service.
- Resolution of internal grievances.
- Sale, transfer, merger, dissolution.
- Determine eligibility of coverage, claims adjudication, subrogation.
- Review of medical necessity, coverage.
- Care coordination and/or case management.
- Others.

(42 CFR 2.33(b), as amended)

SUBPOENAS AND ORDERS

May disclose SUD info if have:

- Subpoena + court order authorizing disclosure.
 - Protect life or serious bodily injury.
 - Extremely serious crime committed by patient.
 - Criminal prosecution.
 - Investigate part 2 program.
- Regulations have specific process for obtaining order, including notice to holder of record.

(42 CFR 2.61-2.67)

- *May need to seek compliant order for certain disclosures.*
- *Must challenge non-compliant subpoena or order.*

NOTICE OF CONFIDENTIALITY PROTECTIONS

- Upon admission (or if patient lacks capacity at the time as soon as patient gains capacity) program must:
 - Communicate federal laws and regulations protecting SUD info.
 - Give patient written summary of laws and regulations, including:
 - Describe limited situations in which part 2 program may acknowledge that patient is present or disclose SUD.
 - State that violation of law is a crime + contact info for reports.
 - State that info related to patients' commission of crime on the part 2 premises or against part 2 personnel is not protected.
 - State that reports of child abuse and neglect are not protected.
 - Cite federal laws and regulations.

(42 CFR 2.22)

PATIENT ACCESS TO RECORDS

- May provide a patient with a copy of or access to the patient's own records.
- No written consent is required to disclose the patient's info to the patient.

(42 CFR 2.23)

But remember:

- HIPAA generally requires "covered entities" to allow patient access to protected health info in a designated set unless exceptions satisfied. (45 CFR 164.524)
- Information Blocking Rule prohibits "actors" from blocking access to electronic health info unless exceptions satisfied. (45 CFR part 171)



SECURITY

- Part 2 programs and lawful holders must have formal policies and procedures to reasonably protect against unauthorized use or disclosure of SUD info or threats to security of SUD info.
- Policies and procedures must address:
 - Transfer and removing records.
 - Destroying records, including sanitizing media.
 - Maintaining records in secure room, locked file cabinet, safe, or similar container or storage facility when not in use.
 - Using and accessing workstations, secure rooms, locked file cabinets, safes, or similar containers or storage facilities.
 - De-identification of records.

(42 CFR 2.16)

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

Substance Abuse Confidentiality x +

samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs

U.S. Department of Health & Human Services



Home | Site Map | Contact Us

Search SAMHSA.gov

Search

Find Treatment | Practitioner Training | Public Messages | Grants | Data | Programs | Newsroom | **About Us** | Publications

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



About Us

Who We Are

Leadership
Regional Administrators
Offices and Centers

Laws and Regulations

Confidentiality Regulations FAQs

Listening Session Comments
on Substance Abuse
Treatment Confidentiality
Regulations

Advisory Councils

Strategic Plan FY2019-FY2023

Accomplishments

Substance Abuse Confidentiality Regulations

Frequently Asked Questions (FAQs) and Fact Sheets regarding the Substance Abuse Confidentiality Regulations.

Fact Sheets regarding the Substance Abuse Confidentiality Regulations

- [Disclosure of Substance Use Disorder Patient Records: Does Part 2 Apply to Me? \(PDF | 1.5 MB\)](#)
 - This fact sheet explains a 42 CFR Part 2 Program and how healthcare providers can determine how Part 2 applies to them.
- [Disclosure of Substance Use Disorder Patient Records: How Do I Exchange Part 2 Data? \(PDF | 1.7 MB\)](#)
 - This fact sheet describes how 42 CFR Part 2 applies to the electronic exchange of healthcare records with a Part 2 Program.

Applying the Substance Abuse Confidentiality Regulations

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

These Frequently Asked Questions (FAQs) are for information purposes only and are not intended as legal advice. Specific questions regarding compliance with federal law should be referred to your legal counsel. State laws may

ADDITIONAL RESOURCES



WWW.HOLLANDHART.COM/ HEALTHCARE

Substance Abuse Confidentiality x Healthcare | Holland & Hart LLP x +

hollandhart.com/healthcare

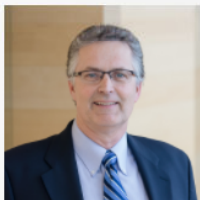


Search by Keyword

OVERVIEW ▶

- PEOPLE
- PRACTICES/INDUSTRIES
- NEWS AND INSIGHTS

CONTACTS



Kim Stanger
Partner
[Boise](#)



Blaine Benard
Partner
[Salt Lake City](#)



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.

 [CLICK HERE FOR COVID-19 RESOURCES FOR HEALTHCARE PROFESSIONALS](#)

The Healthcare Industry is poised to continue its rapid evolution. With this sector now making up close to 20 percent of GDP, our lawyers stand ready to help as changes unfold.

Issues such as rising healthcare costs, healthcare reform, data and privacy security, and innovations in healthcare delivery, device and pharmaceutical designs are forefront in the minds of many of our clients. We are here to guide our clients through the challenges and opportunities that arise in this dynamic industry.

Clients We Serve

- Hospitals
- Individual medical providers
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)

Webinars and Publications

- Owners of healthcare assets
- Imaging centers
- Ambulatory surgery centers
- Medical device and life science companies
- Rehabilitation centers

QUESTIONS?



Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com



Ally Kjellander

Office: (208) 383-3930

aakjellander@hollandhart.com