

HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION



KIM C. STANGER

(6-23)

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. This year, the Idaho Business Review listed him as one of the Leaders in the Law. He is a member of the American Health Law, Past President of the Idaho Bar Association Health Law Section, and a frequent author and speaker on health law-related issues.

DISCLAIMER

This presentation is 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.

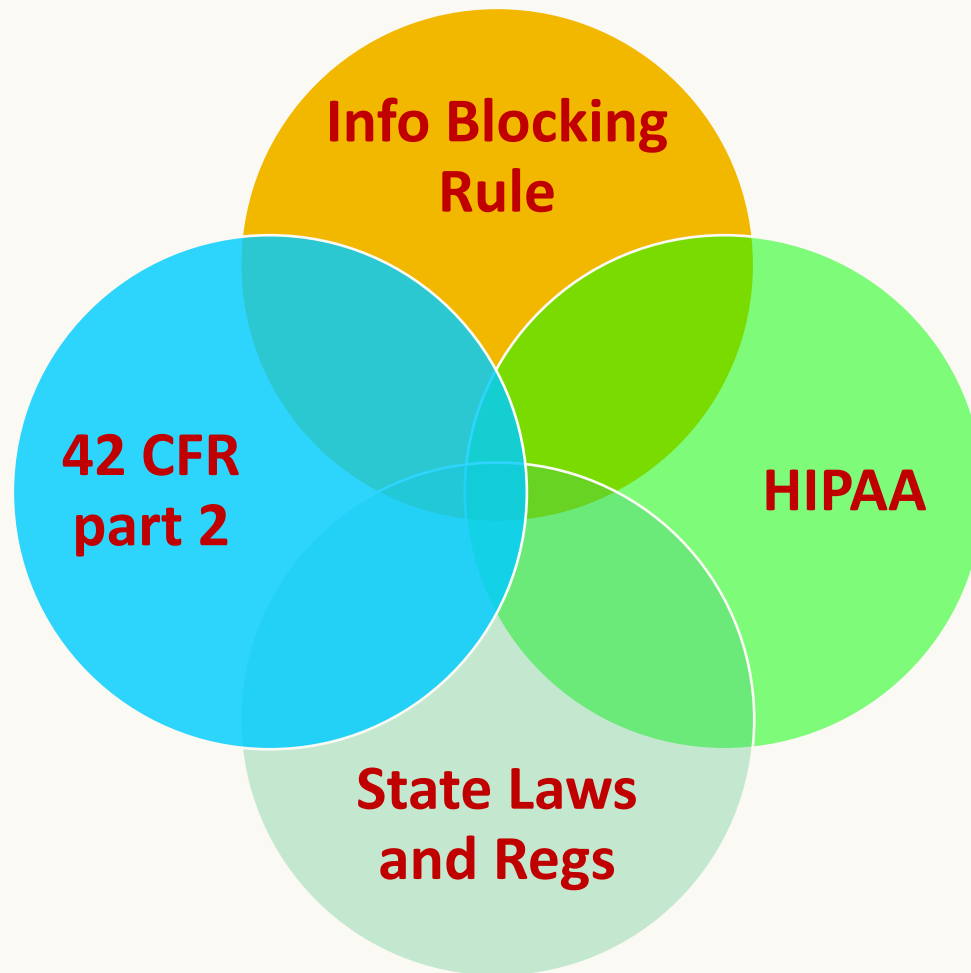
PRELIMINARIES

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

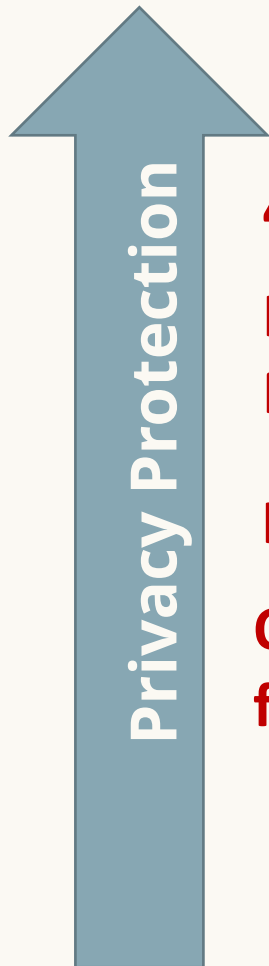
WRITTEN RESOURCES

- Stanger, *Complying With HIPAA: A Checklist for Covered Entities*, <https://www.hollandhart.com/hipaa-checklist-covered-entities>
- Stanger, *Complying With HIPAA: A Checklist for Business Associates*, <https://www.hollandhart.com/checklist-for-business-associates>
- Stanger, *Responding to HIPAA Breaches*, <https://www.hollandhart.com/responding-to-hipaa-breaches>

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)

ENFORCEMENT

- Must self-report breaches of unsecured protected health info
 - To affected individuals.
 - To HHS.
 - To media if breach involves > 500 persons.
- In future, individuals may recover portion of penalties or settlement.
 - On 4/6/22, HHS issued notice soliciting input. (87 FR 19833)
- 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 that—
 - 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

*Presume
PHI
protected
by HIPAA*

(45 CFR 160.103, 164.514)

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 GOVT 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, 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.

(45 CFR 164.502(g))

- 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))



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:

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.
 - OCR 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.

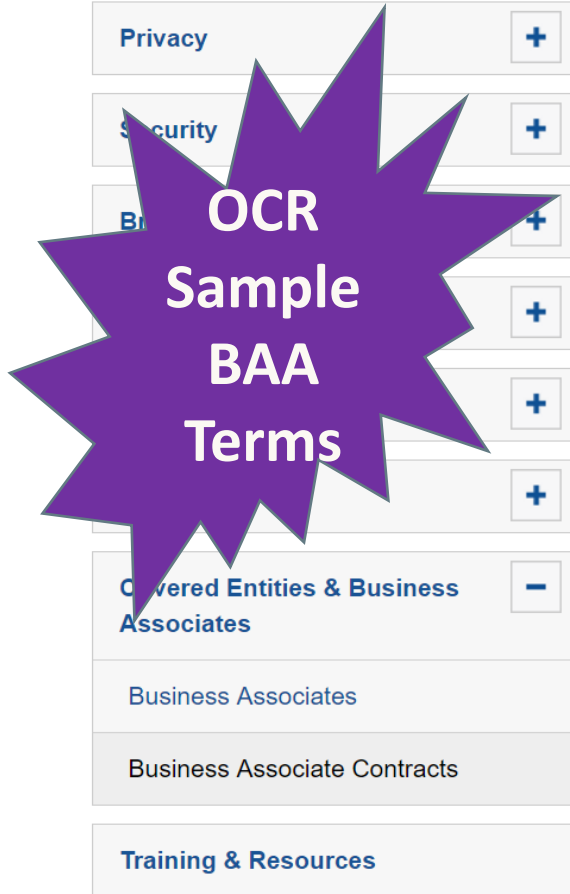
(45 CFR 160.103)

- 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)



OCR
Sample
BAA
Terms

- HIPAA for Professionals
- Privacy +
- Security +
- Business Associates +
- Business Associate Contracts +
- 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.)




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   

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

**Required
Reading!**

PATIENT REQUEST 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*)

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 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.*

OCR GUIDANCE RE REPRODUCTIVE RIGHTS

- On 6/29/22, OCR issued post-*Dobbs* guidance on disclosing PHI relating to reproductive rights.
 - HIPAA prohibits disclosures without patient's authorization unless exception applies.
 - Potential exceptions might include the following; however, HIPAA does not require disclosures in these situations:
 - Disclosures required by law
 - Disclosures for law enforcement purposes.
 - Disclosures to avert serious and imminent threat of harm.
 - **But other laws might require disclosures...**

(<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html>)

HIPAA: PROPOSED RULES

- On 4/17/23, OCR proposed rule that would prohibit covered entities and business associates from using and disclosing PHI for following purposes:
 - Criminal, civil or administrative investigation or proceeding against individuals for seeking, obtaining, providing or facilitating reproductive healthcare that is lawful under the circumstances in which it is provided; or
 - Identification of any person for the purpose of initiating such investigation or proceeding.

(88 FR 23506)

For example, rule would apply if:

- Person seeks care in other state in which care is lawful.
- Person seeks care that is permitted by EMTALA.

OCR GUIDANCE RE ONLINE TRACKING

- On 12/1/22, OCR issued Guidance re Online Tracking Technologies
 - Tracking technologies may collect and analyze info about how users interact with websites and apps.
 - Covered entities and business associates “are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.”
 - May use for treatment, payment and healthcare operations.
 - May only use minimum necessary for permitted purpose.
 - May not use for marketing, vendor’s own research or use, etc., without patient’s HIPAA-compliant authorization.
 - Must have BAA with vendor for permissible uses of PHI.

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

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)

 **NEW:** Health IT Feedback Portal



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

Connect with us:


[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) requires that health care entities and its business associates conduct a risk assessment to identify and protect against risks to the security of electronic protected health information (ePHI). A risk assessment helps your organization ensure it is complying with the HIPAA Security Rule's **technical safeguards**. A risk assessment also helps reveal areas where your organization's ePHI could be at risk. To learn more about the benefits your organization, visit the [Office for Civil Rights](#).

What is the Security Risk Assessment Tool?

The Office of the National Coordinator for Health Information Technology, in collaboration with the HHS Office for Civil Rights (OCR), developed the Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help health care providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

[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 tablet. 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



**Risk
Assessment
Tool**

Need

Please
comm
SRA To
Feedba
trouble
proble
itself. A
any su
improv

You ma
our He
302-47

Subm

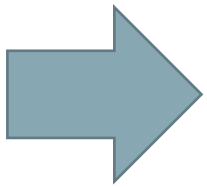
SRA V

[WWW.HHS.GOV/HIPAA/FOR-PROFESSIONALS/SECURITY/GUIDANCE/INDEX.HTML](https://www.hhs.gov/hipaa/for-professionals/security/guidance/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 **A A A** | 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")

HIPAA SECURITY RULE

- In 1/21, HITECH Act amendments required OCR to take into consideration an entity's compliance with recognized security practices (RSPs) when considering HIPAA penalties.
- On 10/31/22, OCR posted a video addressing RSPs available at <https://www.youtube.com/watch?v=e2wG7jUiRjE>:
 - Compliance with RSPs is not a safe harbor but is a factor OCR considers when determining penalties.
 - RSPs =
 - NIST Framework
 - HICP technical volumes
 - Other

<https://www.youtube.com/watch?v=e2wG7jUiRjE>

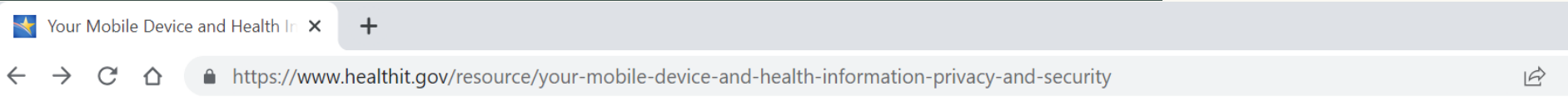
RSP Resources

- **Public Law 116-321:**
 - <https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf>
- **HHS Resources on Section 405(d) of the Cybersecurity Act of 2015:**
 - Health Industry Cybersecurity Practices: Managing Threats and Protecting Patient Data (HICP)
 - <https://405d.hhs.gov/Documents/HICP-Main-508.pdf>
 - <https://405d.hhs.gov/Documents/tech-vol1-508.pdf>
 - <https://405d.hhs.gov/Documents/tech-vol2-508.pdf>
- **NIST Cybersecurity Framework:**
 - <https://www.nist.gov/cyberframework>
- **NIST Online Informative References (OLIR):**
 - <https://csrc.nist.gov/projects/olir>

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)



- TOPICS
- BLOG
- NEWS
- DATA
- ABOUT ONC

Search

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 their mobile devices.



This tool was developed from the experiences of Regional Extension Center staff in the performance of technical assistance to primary care providers. The information contained in this guide is not intended to serve as legal or financial advice. It is not a substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information provided herein.

This web site to any specific resources, tools, products, process, service, manufacturer, or company does not constitute its endorsement by the U.S. Government or the U.S. Department of Health and Human Services.

Resource Link
[Your Mobile Device and Health Information Privacy and Security](#)

Audience
Providers & Professionals

Resource Topics

TELEHEALTH PLATFORM

- Telehealth platforms and services must comply with HIPAA privacy and security rules

(45 CFR part 164)

- During PHE, providers were allowed to use non-compliant technologies (e.g., FaceTime, Messenger, Zoom, Skype, etc.).

(<https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf>)

- OCR confirmed that relaxed security standards will end May 11 but OCR will give 90-day transition period to **August 9, 2023**.

(<https://www.hhs.gov/about/news/2023/04/11/hhs-office-for-civil-rights-announces-expiration-covid-19-public-health-emergency-hipaa-notifications-enforcement-discretion.html>)

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...



Cyberattack forces Idaho hospital to send ambulances elsewhere

By [Sean Lyngaas](#), CNN

Published 5:33 PM EDT, Wed May 31, 2023



<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>



- *Knowledge on Demand* training
- Health Industry *Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP) (2023 edition)

Security Task Force Provides New Resources to Help Address Rising Threat of Cyberattacks in Health and Public Health Se...



FOR IMMEDIATE RELEASE
April 17, 2023

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

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

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.CISA.GOV/STOPRANSOMWARE](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



WHAT IS RANSOMWARE?

LEARN MORE

HAVE YOU BEEN HIT BY RANSOMWARE?

LEARN MORE

Known Exploited Vulnerabilities Catalog

cisa.gov

UPdated

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Locum Tenens Billi....pdf

Show all

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

[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](#)

Text Resize **A A A** Print Share

Health Sector Cybersecurity Coordination Center (HC3)

A Prescription for Health Sector Cybersecurity

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



HC3 Products

Threat Briefs

Highlights relevant cybersecurity topics and raise the HPH sector's situational awareness of current cyber threats, threat

Sector Alerts

Provides high-level, situational background information and context for technical and executive audiences. Designed to assist

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

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 displaying the HHS Breach Portal. The page title is "U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". Below the header, there are navigation buttons for "Under Investigation", "Archive", and "Help for Consumers". A paragraph explains that as required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches affecting 500 or more individuals. The page is titled "Cases Currently Under Investigation" and lists breaches reported within the last 24 months. A table titled "Breach Report Results" contains the following data:

| Expand All | Name of Covered Entity | State | Covered Entity Type | Individuals Affected | Breach Submission Date | Type of Breach | Location of Breached Information |
|------------|------------------------------------|-------|---------------------|----------------------|------------------------|---------------------|----------------------------------|
| + | Julieta Y. Echeverria D.D.S., Inc. | CA | Healthcare Provider | 529 | 05/20/2022 | Theft | Paper/Films |
| + | Bryan County Ambulance Authority | OK | Healthcare | 14273 | 05/18/2022 | Hacking/IT Incident | Network Server |

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.*

IN OTHER NEWS...



DATA PRIVACY LAWS



- Watch for data privacy developments.
 - Several federal bills have been proposed.
 - Cyber Incident Reporting Critical Infrastructure Act of 2022 (CIRCI) regulations are pending.
 - Will require reports of cybersecurity breaches.
- Beware state privacy laws.
 - See, e.g.,
<https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

FTC PRIVACY LAWS

Unfair Trade Practices Act § 5

- Prohibits unfair or deceptive acts affecting commerce.

(15 USC 45)

- FTC take position that failing to protect data may violate act, e.g.,
 - Contrary to representations, or
 - Failure to implement reasonable security and privacy measures.

FTC Health Breach Notification Rule

- Requires vendors of personal health records to notify individuals after a breach.

(16 CFR part 318)

- FTC has proposed amendments to rules.
 - Extends to health apps.
 - Confirms “breach” includes unauthorized access or disclosure.

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)

42 CFR PART 2 SUBSTANCE USE RECORDS

On 11/28/22, HHS proposed new rules to implement CARES Act 3221 to more fully align Part 2 with HIPAA.

- Permits use and disclosure of Part 2 records based on a single patient consent given once for all future uses and disclosures for treatment, payment, and health care operations.
- Permits redisclosure of Part 2 records in any manner permitted by the HIPAA Privacy Rule, with certain exceptions.
- Expands prohibitions on use and disclosure of Part 2 records in civil, criminal, administrative, and legislative proceedings.
- Provides for civil money penalties for violations of Part 2.
- Updates breach notification requirements.
- Updates HIPAA Notice of Privacy Practices requirements to address Part 2 records and individual rights.

(87 FR 74216)

- **Watch for final rules.**

ADDITIONAL RESOURCES



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

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other



Holland & Hart

People Capabilities

Search by keyword

Healthcare

Overview Expertise People News and Insights

Areas of Focus

Business Litigation Corporate Employment and Labor Mergers and Acquisitions Real Estate

Healthcare is a massive industry that needs specialized legal advice.

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

QUESTIONS?



Kim C. Stanger
Office: (208) 383-3913
Cell: (208) 409-7907
kcstanger@hollandhart.com