

HIPAA Privacy and Breach Notification Rules



Kim C. Stanger

(4/25)

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

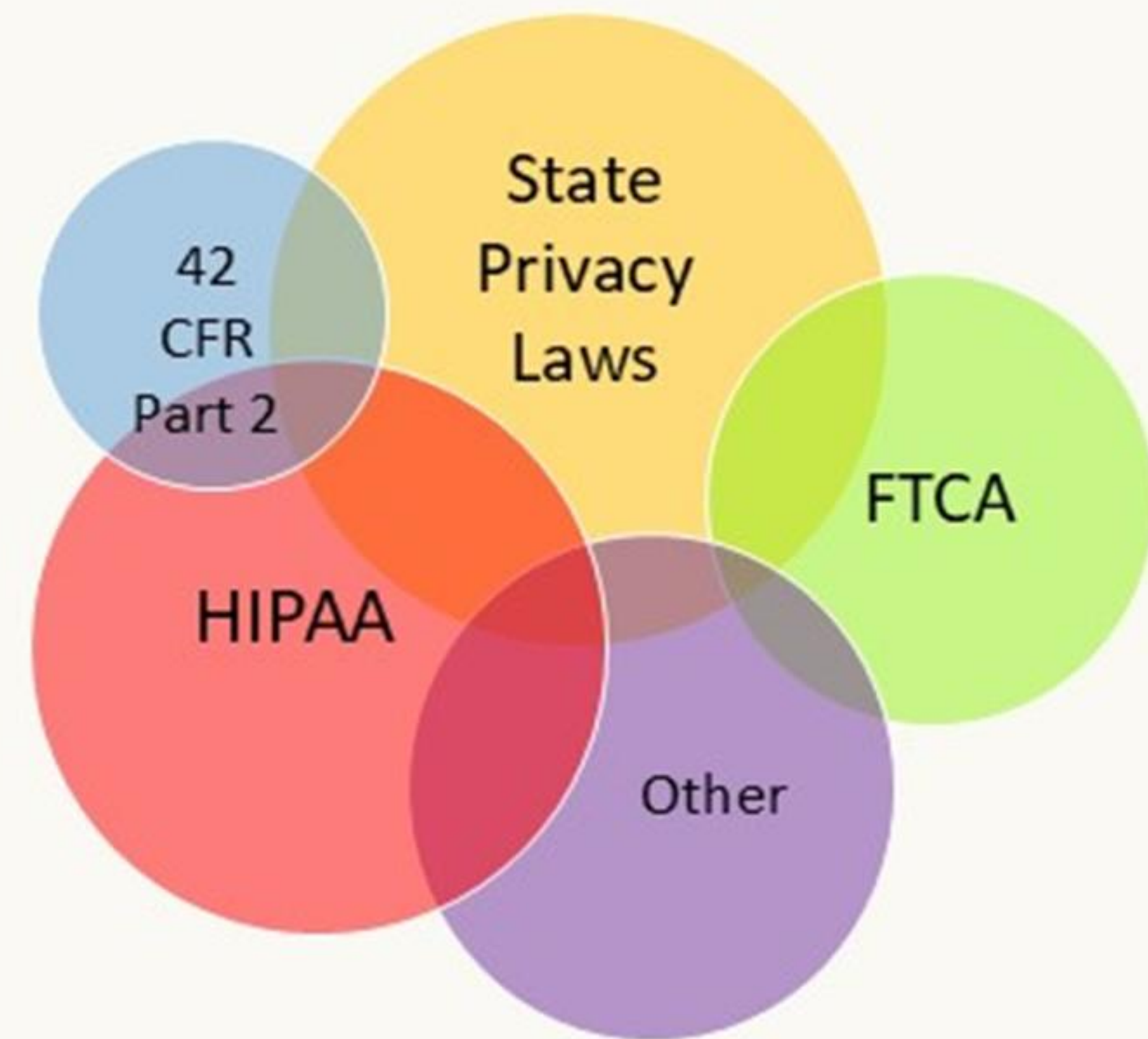
- Stanger, *Complying With HIPAA: A Checklist for Covered Entities*,
<https://www.hollandhart.com/hipaa-checklist-covered-entities>
- Stanger, *Complying With HIPAA: A Checklist for Business Associates*,
<https://www.hollandhart.com/checklist-for-business-associates>
- Stanger, *Responding to HIPAA Breaches*,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

Privacy Laws

Privacy Protection

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

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



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">• \$141* to \$71,162* per violation• Up to \$2,134,831* 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">• \$1,424* to \$71,162* per violation• Up to \$2,134,831* per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none">• \$14,232* to \$71,162* per violation• Up to \$2,134,831* per type per year• Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none">• \$71,162 to \$2,134,831* per violation• Up to \$2,134,831* per type per year• Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

Recent HIPAA Resolutions

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

Date	Conduct	Resolution
10/31/24	Ambulance services hit with ransomware attack.	\$90,000
10/31/24	Plastic surgeons hit with ransomware attack.	\$500,000
10/17/24	Dentist office failed to provide timely access to records.	\$70,000
10/3/24	Hospital hit with ransomware attack.	\$240,000
9/26/24	Eye and Skin Center hit with ransomware attack.	\$250,000
8/1/24	EMS provider failed to provide timely access to records.	\$115,200
7/1/24	Health system hit with ransomware attack.	\$950,000
4/1/24	Essex Residential Care failed to provide timely access to records.	\$100,000
3/29/24	Phoenix Healthcare failed to provide timely access to records.	\$35,000
2/6/24	Montefiore Medical Center failed to protect against malicious insider selling info.	\$4,750,000
11/20/23	St. Joseph's Medical Center disclosed PHI to news reporter.	\$80,000
10/31/23	Doctor's Management Services hit by ransomware affecting 206,695 persons.	\$100,000
9/11/23	L.A. Care Plan failed to secure patient portal, perform risk analysis, and mailed ID cards to wrong patients. Affected 2500+ persons.	\$1,300,000
8/24/23	UnitedHealthcare failed to timely provide copy of records.	\$80,000
6/28/23	iHealth Solutions' PHI of 267 persons was exfiltrated by unauthorized persons.	\$75,000

Top HIPAA Risks

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



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
 - 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., 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

Presumably PHI

(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 health care 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 without authorization.

➤ *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)

Required by Law

- May use or disclose PHI to the extent disclosure is required by law.
 - Must limit to requirements of the law.
 - Does not apply if law only allows disclosure.

(45 CFR 164.512(a))

Serious and Imminent Harm

- May use or disclose PHI if have good faith belief that use or disclosure is:
 - Necessary to prevent or lessen a serious imminent threat to the health or safety of a person or the public; and
 - To a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
 - Good faith presumed if based on knowledge or credible representation by person with knowledge.

(45 CFR 164.512(j))

Public Health Activities

- May use or disclose PHI for certain public health activities.
 - To report child abuse or neglect.
 - To report adult abuse or neglect if certain conditions are satisfied.
 - To public health authority authorized to receive info to prevent disease or injury.
 - To a person at risk of contracting or spreading disease if covered entity is authorized by law to contact person.
 - To report school immunizations subject to conditions.
 - For certain workplace surveillance required by regulations.
 - For certain FDA-related actions.

(45 CFR 164.512(b)-(c))

Health Oversight Activities

- May disclose PHI to health oversight agency for oversight activities authorized by law.
 - Includes audits; investigations; inspections; or civil, criminal, or administrative proceedings.
 - Relates to
 - Oversight of health care system.
 - Eligibility for benefits under gov't programs.
 - Compliance with gov't programs.
 - Compliance with civil rights laws.

(45 CFR 164.512(d))

Judicial and Administrative Proceedings

- May disclose PHI if—
 - Order signed by judge or administrative tribunal.
 - Subpoena, discovery request, or legal process not accompanied by court order if:
 - Obtain written assurances from party issuing subpoena that either:
 - Patient has been notified and had chance to object, or
 - Reasonable steps taken to obtain a protective order.
 - Take reasonable steps to notify the patient yourself.

Best
Option

(45 CFR 164.512(e))

Law Enforcement: Legal Process

- May disclose PHI per
 - Court order, warrant, subpoena or summons issued by a judicial officer (i.e., judge or magistrate).
 - Grand jury subpoena.
 - Administrative request, subpoena, summons or demand authorized by law if:
 - PHI relevant and material to legitimate law enforcement inquiry;
 - Request is reasonably specific and limited to purpose; and
 - De-identified info could not be used.

(45 CFR 164.512(f)(1))

Law Enforcement: No Legal Process

- May disclose PHI to law enforcement if:
 - Report crime on the premises.
 - Request by law enforcement to identify or locate suspect, fugitive, witness or missing person.
 - Disclose only limited PHI.
- Request by law enforcement about victim of crime, and
 - Victim agrees, or
 - Victim unable to agree and law enforcement represents that PHI needed to determine violation of law by someone other than the patient and PHI will not be used against person, info needed immediately, and disclosure in best interests of individual.
- Person in custody and info needed:
 - To provide healthcare to person, or
 - For health and safety of others.

(45 CFR 164.512(f)(1))

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (*HIPAA*) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and

others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Workers Comp

- May disclose PHI as authorized and to the extent necessary to comply with workers comp laws.

(45 CFR 164.512(l))

Other Exceptions

- To coroners
- To funeral directors
- For organ donation
- For certain research purposes
- For military personnel
- For national security and intelligence purposes

(45 CFR 164.512(g)-(k))

Reproductive Rights Rule



The Background

OCR concerned about disclosing RPHI if:

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



Reproductive Health Care Info (“RPHI”)

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

- Broader than just abortion; extends to any PHI re reproductive healthcare.

(45 CFR 160.103)

- Applies to any provider or business associate who has RPHI, not just the provider who rendered the reproductive healthcare.

(45 CFR 164.502)

Reproductive Health Rule

- If reproductive healthcare was legal where it was obtained, covered entities and business associates may not use or disclose RPHI for purposes of criminal, civil or administrative investigation or to impose liability.

(45 CFR 164.502(a)(5))

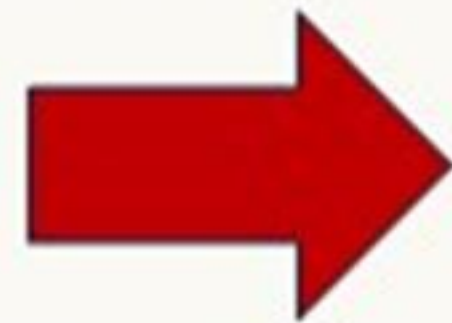
- Must obtain attestation from persons seeking RPHI for purposes of criminal, civil or administrative investigation or liability to confirm purpose and legality.

(45 CFR 164.509)

- ✓ Ability to use or disclose depends on the purpose for which info is sought, not necessarily its status as RPHI.

Reproductive Health Rule: Required Attestation

Covered entity or business associate may not use or disclose reproductive care PHI for **these purposes** without first obtaining a required attestation from the person seeking the PHI. (45 CFR 164.509)



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

Reproductive Rights Rule: Required Attestation

Valid attestation =

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

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

OCR Model Attestation

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



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

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

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

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

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

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

Model Instructions

Information for the Person Requesting the PHI

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

¹ See 45 CFR 160.103 (definition of "Covered entity").

² See 45 CFR 160.103 (definition of "Business associate").

³ See 45 CFR 160.103 (definition of "Protected health information").

⁴ See 45 CFR 160.103 (definition of "Reproductive health care").

⁵ See 45 CFR 164.512(d).

⁶ See 45 CFR 164.512(e).

⁷ See 45 CFR 164.512(f).

⁸ See 45 CFR 164.512(g)(1).

⁹ See 45 CFR 164.502(a)(5)(ii)(A).

¹⁰ See 45 CFR 164.502(a)(5)(ii)(B), (C). For more information on the presumption and when it applies, see 45 CFR 164.502(a)(5)(ii)(C).

¹¹ See 42 U.S.C. 1320d-6.

¹² See 45 CFR 164.509(b)(3) and (c)(iv).

Reproductive Rights Rule: Future is Unclear

Case 5:24-cv-00204-H Document 1 Filed 09/04/24 Page 1 of 16 PageID 1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
LUBBOCK DIVISION

STATE OF TEXAS,
Plaintiff,

v.

UNITED STATES DEPARTMENT OF
HEALTH AND HUMAN SERVICES;
XAVIER BECERRA, in his official capacity
as Secretary of the United States
Department of Health and Human Services;
MELANIE FONTES RAINER, in her
official capacity as Director of the
Department of Health and Human Services
Office for Civil Rights,
Defendants.

CIVIL ACTION No. _____



TEXAS'S ORIGINAL COMPLAINT

1. Texas brings this action seeking declaratory and injunctive relief against enforcement of two final rules issued by the United States Department of Health and Human Services.

Holland & Hart

Patient Authorizes Disclosure

- Written requests
- Authorizations



Patient Request to Provide ePHI

- Must provide electronic PHI in designated record set to third party if:
 - Written request by patient;
 - Clearly identifies the designated recipient and where to send the PHI; and
 - Signed by patient.
- (45 CFR 164.524(c)(3)(ii))
- Part of individual's right of access.
 - Must respond within 30 days.
 - May only charge reasonable cost-based fee.

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

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 generally 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:
 - 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,

Not defined as
“Marketing”

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

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

Sale of PHI

- Cannot sell PHI unless obtain patient's prior written authorization and the authorization discloses whether covered entity will receive remuneration in exchange for PHI.
- "Sale of PHI" = disclosure of PHI by covered entity or business associate if they receive (directly or indirectly) any remuneration (financial or otherwise) from or on behalf of the recipient of the PHI in exchange for the PHI.

(45 CFR 164.508(a)(4))

- May apply to charging excessive fees to copy or produce records

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

Fundraising

- Generally need authorization to use or disclose PHI for fundraising unless you:
 - Disclose limited PHI to institutionally-related foundation or business associate,
 - Name, address, contact info, age, gender and birth date.
 - Dates of healthcare provided by covered entity.
 - Department of service.
 - Treating physicians.
 - Outcome information.
 - Health insurance status.
 - Include statement in notice of privacy practices, and
 - With each fundraising communication, provide clear and conspicuous opportunity to opt out of fundraising, which method may not cause undue burden or more than nominal cost.

(45 CFR 164.514(f))

Research

- Need authorization for most research purposes.
 - No expiration date on authorization.
 - May condition authorization on research-related treatment.
- Do not need authorization if:
 - Obtain approval of Institutional Review Board, or
 - Privacy Committee.
- See OCR, *HIPAA and Research*, available at www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/

(164.512(i) and elsewhere)

Parents and Personal Representatives



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))

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))

✓ *Beware State laws.*

Family Members and Personal Reps

- Potential bases for disclosure
 - Personal rep has right to access PHI.
 - Disclosure for treatment, payment or health care operations.
 - Disclosure to family members or others involved in care or payment if:
 - Patient did not object,
 - In patient's best interests, and
 - Limit disclosure to scope of person's involvement.
 - Other exception, e.g., to avert serious threat.
- See OCR, *Communicating with a Patient's Family, Friends or Others*, available at www.hhs.gov/ocr/privacy/hipaa.



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.

Business Associates



Business Associates

- May disclose PHI to business associates if have valid business associate agreement (“BAA”).
 - Covered entity – business associate
 - Business associate – subcontractor business associate
- (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); see also

https://www.hollandhart.com/checklist_for_hipaa_business_associate_agreements)

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

Not Business Associates

- Members of covered entity's workforce.
 - Covered entity has control over the person.
- Entities who do not handle PHI as part of their job duties.
 - Janitor, mailman, some vendors, etc.
- Entities that receive PHI to perform functions on their own behalf, not on behalf of covered entity.
 - E.g., banks, third-party payors, etc.
- Other healthcare providers while providing treatment.
- Data transmission companies that do not routinely access PHI.
 - Entity is mere “conduit” of PHI.
- Members of an organized healthcare arrangement.
 - Group of entities that provide coordinated care.

(See <https://www.hollandhart.com/avoiding-business-associate-agreements>)

<https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>

HIPAA for Professionals

Privacy



Security



Br



OCR
Sample
BAA
Terms



Business Associates & Business



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

Liability for Acts of Business Associate or Subs

- Per federal common law of agency:
 - Covered entity may be liable for acts of business associate, and
 - Business associate may be liable for acts of subcontractor.

(45 CFR 160.402(c))
- Test: right or authority of a covered entity or business associate to control the conduct.
 - Contract terms.
 - Right to give interim directions or control details.
 - Relative size or power of the entities.
- *Maintain independent contractor status!*

(78 FR 5581-82)

Making the Disclosure



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 accompanying a subpoena, or representations from police that they need info for immediate identification purposes.

(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.
- May rely on judgment of:
 - Another covered entity.
 - Professional within the covered entity.
 - Business associate for professional services.
 - Public official for permitted disclosure.

(45 CFR 164.502 and .514)

Patient Rights



Notice of Privacy Practices

- Notice summarizes HIPAA rules and explains how you will use the patient's information.
 - Must contain certain provisions.
(See <https://www.hollandhart.com/checklist-for-hipaa-notice-of-privacy-practices>)
- Direct treatment providers:
 - Give copy to patients by first date of treatment.
 - Post notice in “prominent locations”
 - Post notice on website.
 - Make good faith attempt to obtain acknowledgment of receipt.

(45 CFR 164.520)
- *Will need to update NPP by 2/26 to accommodate new rules.*

Request Restrictions on Use or Disclosure

- Individual has right to request additional restrictions on use or disclosure for treatment, payment and operations.
- Covered entity may generally decline restrictions.
 - *Don't agree!*
 - Beware situations where you ask for permission to disclose.
- If covered entity agrees to additional restrictions, it must abide by them unless:
 - Emergency, or
 - Disclosure required by regulations.
- Covered entity may terminate the agreement for additional restrictions prospectively.

(45 CFR 164.522)

Restrictions on Disclosure to Insurers

- Must agree to patient's request to restrict disclosure of PHI to a health plan if:
 - PHI pertains to health care item or service for which the patient, or another person on the patient's behalf, paid the covered entity in full; and
 - Disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law.

(45 CFR 164.522)

✓ *Generally, don't ask the patient unless you want to allow patient to be self-pay.*

Request Alternative Communications

- Must accommodate reasonable request to receive PHI by alternative means or at alternative locations.
 - May require written request.
 - May not require explanation.
 - May require information as to how payment will be handled.

(45 CFR 164.522(b))

Communicating by E-mail or Text

- HIPAA Privacy Rule allows patient to request communications by alternative means or at alternative locations.
 - Including unencrypted e-mail.

(45 CFR 164.522(b))

- Omnibus Rule commentary states that covered entity or business associate may communicate with patient via unsecured e-mail so long as they warn patient of risks and patient elects to communicate via unsecured e-mail to text.

(78 FR 5634)

- Does not apply to disclosures between your employees or providers.

Right to Access PHI

- Individual has right to inspect and obtain copy of PHI in “designated record set”
 - Documents used to make decisions re healthcare or payment.
 - **Includes documents created by others.**
- Exceptions: no right to access – –
 - info outside designated record set, e.g., peer review, etc.
 - psychotherapy notes.
 - info in anticipation of legal action.
 - info provided under promise of confidentiality.
 - info if access would cause substantial harm to patient or other, subject to review by independent provider.
- Must respond within 30 days; may get 30-day extension.

(45 CFR 164.524)

www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Required Reading!

HHS.gov

Health Information Privacy

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

HIPAA for Professionals

Privacy

[Summary of the Privacy Rule](#)

[Guidance](#)

[Combined Text of All Rules](#)

Security

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

Right to Access PHI

- Must provide in form requested if readily produceable.
- May not impose unreasonable barrier to access
 - Beware Information Blocking Rule.
- May charge reasonable cost-based fee if notify in advance, e.g.
 - Labor for copying (photocopying, scanning, converting to format requested, transferring to e-mail, mailing or e-mailing).
 - Supplies for creating paper (paper, toner) or electronic media (CD, USB).
 - Postage.
 - Preparation of summary if agreed by patient.
- May not include cost of:
 - Reviewing, verifying, or documenting request.
 - Searching, retrieving, or compiling records.
 - Maintaining system, data access, storage or infrastructure.

(45 CFR 164.524; <https://www.hollandhart.com/charging-patients-for-copies-of-their-records-ocr-guidance>)

Right to Access PHI

- If covered entity denies the request:
 - Must give access to other info to the extent able.
 - Must provide written explanation, including:
 - Basis for denial.
 - Right to submit denial to independent review (if applicable).
 - Right to complain to covered entity, including the name, title and phone number to whom complaints are directed.
 - If the covered entity does not maintain the info, it must tell the patient where the info is located.

(45 CFR 164.524)

Right to Access PHI: Send PHI to Third Party

- Patient has right to direct that PHI be sent to third party.
- Request must:
 - Be in writing (e.g., paper, electronic, portal)
 - Signed by patient or personal rep
 - Clearly identify the recipient
 - Clearly identify where records to be sent.

(45 CFR 164.524)

- Limits applicable to patient apply to such requests.
 - Must respond within 30 days.
 - Must provide in form and format requested.
- Must take reasonable steps to protect the PHI in transit.

(OCR Guide to Patient Access)

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*)

Right to Request Amendment

- Individual has right to request amendment.
- Covered entity may deny request if:
 - Record not part of designated record set.
 - Entity did not create the record unless creator is no longer available.
 - Record not subject to access.
 - Record is accurate and complete.
- Must act on request within 60 days.
 - May obtain a 30-day extension.
- Additional rules depend on whether request is accepted or denied.

(45 CFR 164.526)

Right to Accounting of Disclosures

- Individual has a right to request accounting of certain disclosures made for prior 6 years.
 - Improper disclosures.
 - Disclosures made per 164.512, e.g.,
 - Required by law.
 - For public health activities.
 - For health oversight activities.
 - For certain law enforcement purposes.
- Accounting must include certain information specified in regs.
- Must respond to request within 60 days.
- May obtain 30-day extension.

(45 CFR 164.528)

Administrative Requirements



Administrative Requirements

- Designate HIPAA privacy and security officers in writing.
- 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)

Other Issues



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.
 - Modifies content of NPP.

(86 FR 6446)

➤ *No final rule yet.*

HIPAA and Online Tracking

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



About HHS Programs & Services Grants & Contracts Laws & Regulation

Health Information Privacy

HIPAA for Individuals

Filing a Complaint

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Privacy](#) > [Guidance Materials](#) > U

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security +

Breach Notification +

Compliance & Enforcement +

Special Topics +

Patient Safety +

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

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

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

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

On March 18, 2024, OCR updated this guidance to increase clarity for regulated entities and the public.

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to

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 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

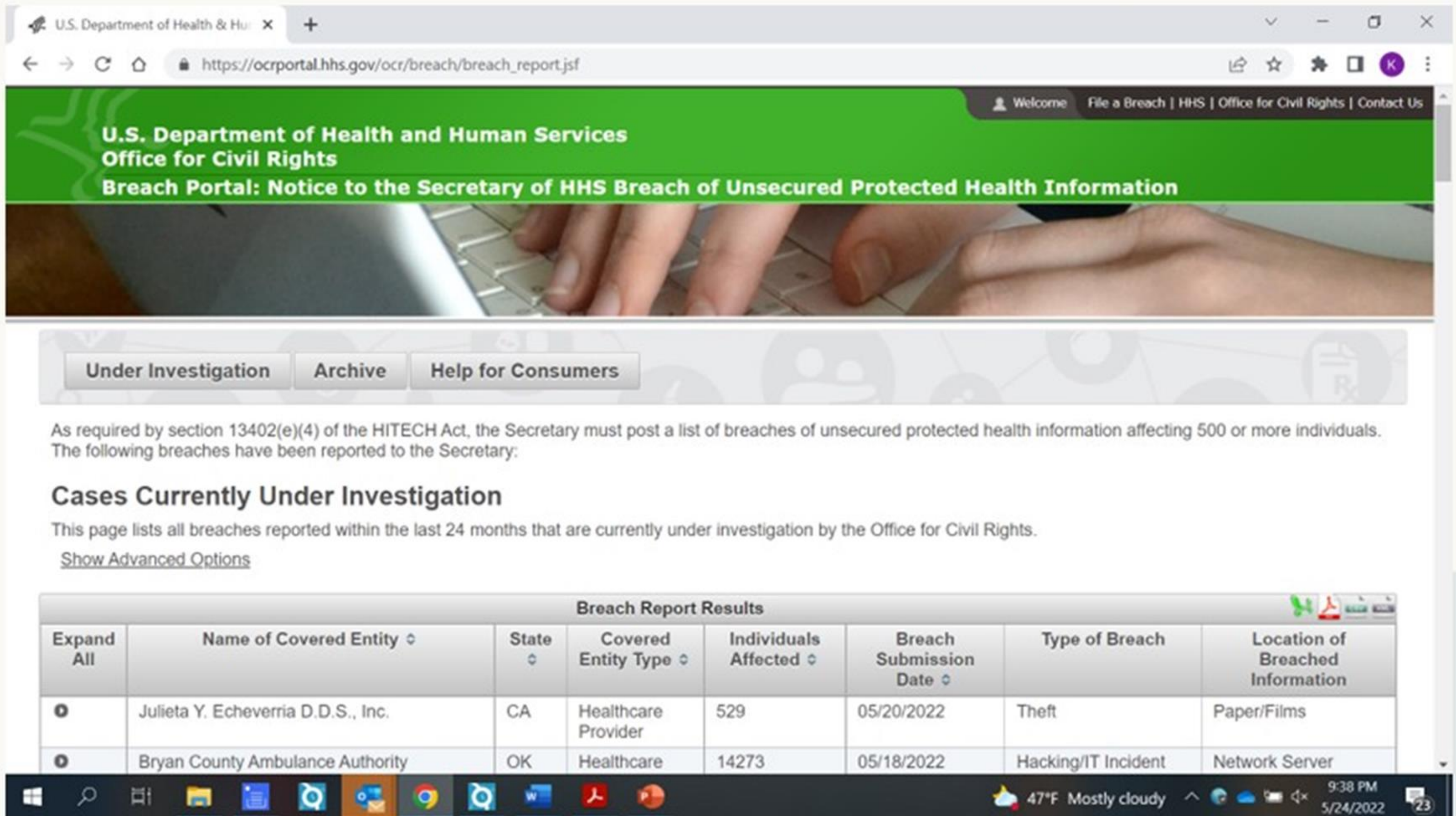
- If breach involves fewer than 500 persons:
 - Submit to HHS annually within 60 days after end of calendar year in which breach was discovered (i.e., by March 1).
- If breach involves 500 or more persons:
 - Notify HHS contemporaneously with notice to individual or next of kin, i.e., without unreasonable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



The screenshot shows the HHS Breach Portal website. The header includes the U.S. Department of Health and Human Services logo and the Office for Civil Rights. The main title is "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". Below the header, there are three tabs: "Under Investigation", "Archive", and "Help for Consumers". The "Under Investigation" tab is selected. The main content area explains that, 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. Below this, there is a section titled "Cases Currently Under Investigation" which lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights. A link "Show Advanced Options" is provided. The table below shows the breach report results for two entities.

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
	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.*

Additional Resources



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

Free content:

- Recorded webinars
- Client alerts
- White papers
- Other



The screenshot shows the Holland & Hart website's Healthcare section. At the top, the navigation bar includes the firm's name, 'People Capabilities', and a search bar. The main header features the word 'Healthcare' in large white text over a dark background with a stethoscope image. Below this is a sub-navigation bar with links for 'Overview', 'Expertise', 'People', and 'News and Insights'. The 'Areas of Focus' section contains five buttons: 'Business Litigation', 'Corporate', 'Employment and Labor', 'Mergers and Acquisitions', and 'Real Estate'. A central text block states: 'Healthcare is a massive industry that needs specialized legal advice. Healthcare spending represents about a fifth of US GDP. Few sectors are as complex and highly regulated. In an ultra-competitive environment, our industry-experienced team takes care of clients' legal issues so they can focus on business. Our team provides holistic guidance on regulatory issues, including Stark, Anti-Kickback Statute, HIPAA, Medicare/Medicaid, and similar state laws. We handle provider and payer contracting; mergers, acquisitions, and joint ventures; data privacy and security; licensing, credentialing and medical staff issues; government investigations and False Claim Act litigation; antitrust and trade regulation; employment; real estate; tax; employee benefits; and administrative or civil litigation. Given our combined experience, there is not much our healthcare clients face that we cannot handle.' To the right, under 'Primary Contacts', is a photo of Kim Stanger. At the bottom, there are three circular icons with corresponding text: a document icon for 'webinar recordings', a book icon for 'PUBLICATIONS' (with a link to health law publications and the Health Law blog), and a caduceus icon for 'IDAHO PATIENT ACT TIMELINE'.

Questions?



Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com