

# HIPAA PRIVACY, SECURITY AND BREACH NOTIFICATION RULES



**KIM C. STANGER**

Compliance Bootcamp

(2-20)

This presentation is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They 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 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.

# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (“HIPAA”)

- 45 CFR 164
  - .500: Privacy Rule
  - .300: Security Rule
  - .400: Breach Notification Rule
- HITECH Act
  - Modified HIPAA
  - Implemented by HIPAA Omnibus Rule

# REMEMBER OTHER LAWS



**More  
restrictive law**

**HIPAA**

**Less restrictive  
law**

- HIPAA preempts less restrictive laws.
- Comply with more restrictive law, e.g.,
  - Idaho hospital regulations (IDAPA 16.03.14.220)
  - Federally assisted drug and alcohol treatment program (42 CFR part 2)
  - State drug and alcohol programs
  - Others, e.g., AIDS/HIV, mental health, etc.?

# CRIMINAL PENALTIES

- Applies if employees or other individuals obtain or disclose protected health info from covered entity without authorization.

Conduct	Penalty
Knowingly obtain info in violation of the law	<ul style="list-style-type: none"><li>• \$50,000 fine</li><li>• 1 year in prison</li></ul>
Committed under false pretenses	<ul style="list-style-type: none"><li>• 100,000 fine</li><li>• 5 years in prison</li></ul>
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	<ul style="list-style-type: none"><li>• \$250,000 fine</li><li>• 10 years in prison</li></ul>

# HIPAA CIVIL PENALTIES

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"><li>• \$119* to \$59,522* per violation</li><li>• Up to \$25,630* per type per year</li><li>• <b>No penalty if correct w/in 30 days</b></li><li>• OCR may waive or reduce penalty</li></ul>
Violation due to reasonable cause	<ul style="list-style-type: none"><li>• \$1,191* to \$59,522* per violation</li><li>• Up to \$102,522* per type per year</li><li>• <b>No penalty if correct w/in 30 days</b></li><li>• OCR may waive or reduce penalty</li></ul>
<b>Willful neglect,</b> but correct w/in 30 days	<ul style="list-style-type: none"><li>• \$11,904* to \$59,522* per violation</li><li>• Up to \$256,305* per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>
<b>Willful neglect,</b> but do not correct w/in 30 days	<ul style="list-style-type: none"><li>• At least \$59,522* per violation</li><li>• Up to \$1,754,698* per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>

(45 CFR 102.3, 160.404; 85 FR 2879)



# 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.*

# ENFORCEMENT

- State attorney general can bring lawsuit.
  - \$25,000 fine per violation + fees and costs
- In future, individuals may recover percentage of penalties.
- Must sanction employees who violate HIPAA.
- Must self-report breaches of unsecured protected health info
  - To affected individuals.
  - To HHS.
  - To media if breach involves > 500 persons.
- Possible lawsuits by affected individuals or others.



# 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 INFORMATION

- Protected health info (“PHI”) =
  - Individually identifiable health info, i.e., info that could be used to identify individual.
  - Concerns physical or mental health, health care, or payment.
  - Created or received by covered entity in its capacity as a healthcare provider.
  - Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.

# NOT COVERED BY HIPAA

- Info after person has been dead for 50 years.
- Info maintained in capacity other than as provider.
  - e.g., as employer
  - *Beware using patient info for employment purposes.*
- “De-identified” info, i.e., remove certain identifiable info
  - Names
  - Dates (birth, admission, discharge, death)
  - 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

***PHI protected  
by HIPAA***

# PROHIBITED ACTIONS

- Cannot use, access or disclose PHI unless:
  - Permitted by HIPAA, or
  - Have patient's or personal rep's authorization.
- Applies to
  - Unauthorized disclosure outside covered entity.
  - Unauthorized use within covered entity.
  - Unauthorized access from within or outside covered entity.

# 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.
- May disclose PHI to another covered entity for other entity's:
  - Treatment;
  - Payment; or
  - Certain healthcare operations if both have relationship with patient.
- Exception: psychotherapy notes.
  - Requires specific authorization for use by or disclosures to others.

(45 CFR 164.506, 164.508 and 164.522)

# TREATMENT, PAYMENT OR OPERATIONS

- If agree with patient to limit use or disclosure for treatment, payment, or healthcare operations, you must abide by that agreement except in an emergency.

(45 CFR 164.506 and 164.522)

- *Don't agree to limit disclosures for treatment, payment or operations.*
  - *Exception: disclosure to insurers; see discussion below.*
- *Beware asking patient for list of persons to whom disclosure may be made.*
  - *Creates inference that disclosures will not be made to others.*
  - *If list persons, ensure patient understands that we may disclose to others per HIPAA.*

# PERSONS INVOLVED IN CARE

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

(45 CFR 164.510)



# FACILITY DIRECTORY

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

(45 CFR 164.510)

# EXCEPTIONS FOR PUBLIC HEALTH OR GOVERNMENT FUNCTIONS

- Another law requires disclosures
- Disclosures to prevent serious and imminent harm.
- 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

# PATIENT REQUESTS TO SEND PHI TO THIRD PARTY

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

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

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

# 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)

# EMPLOYMENT PHYSICALS, DRUG TESTS, OR IMES

- HIPAA generally applies to employment physicals, drug tests, school or physicals, independent medical exams (“IME”), etc.
  - Obtain patient’s authorization to disclose before providing service.
  - Provider may condition exam on authorization.
  - Employer may condition employment on authorization.

(65 FR 82592 and 82640)

- Generally may not use PHI obtained in capacity as healthcare provider for employment-related decisions.

(67 FR 53191-92)

- Possible exceptions:
  - Disclosure to avoid serious and imminent threat of harm.
  - Disclosures required by OSHA, MSHA, etc.
  - Workers compensation

# MARKETING

- Generally need authorization if communication is 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 of patient, 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))

# 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)

# 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))

- 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)



# DIVORCED PARENTS

- Non-custodial parent is entitled access info, but must redact address info if custodial parent requests same in writing.

(IC 32-717A)

# PERSONAL REPRESENTATIVES

- Not required to treat personal rep as patient (i.e., do not 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.

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

provider\_ffg.pdf  
https://www.hhs.gov/sites/default/files/provider\_ffg.pdf



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



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

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

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

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.<sup>2</sup>

#### COMMON QUESTIONS ABOUT HIPAA

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

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

Here are some examples:

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

# BUSINESS ASSOCIATES

- May disclose PHI to business associates if have valid business associate agreement (“BAA”).
- Failure to execute BAA = HIPAA violation
  - May subject you to HIPAA fines.
    - Recent settlement: gave records to storage company without BAA: \$31,000 penalty.
  - Based on recent 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)

Business Associate Contr X

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

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



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

top

# LIABILITY FOR ACTS OF BUSINESS ASSOCIATE OR SUBS

- Covered entity or business associate:
  - Knows that business associate or subcontractor is violating HIPAA, and
  - Fails to take action to end the violation or terminate the BAA.

(45 CFR 164.504(e)(1))

- Business associate or subcontractor is acting as agent of the covered entity within the scope of the agency.
  - Test: right of control
  - *Maintain independent contractor status!*

(45 CFR 160.402(c)).

# 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)

# MINIMUM NECESSARY STANDARD

- Must adopt policies addressing—
  - Internal uses of PHI:
    - Identify persons who need access.
    - Draft policies to limit access accordingly.
  - External disclosures of PHI:
    - Routine disclosure: establish policies.
    - Non-routine disclosures: case-by-case review.
  - Requests for PHI:
    - Routine requests: establish policies.
    - Non-routine requests: case-by-case review.

# HIPAA SECURITY RULE

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

## Protect ePHI:

- Confidentiality
- Integrity
- Availability

# RISK ASSESSMENT

ov/providers-professionals/security-risk-assessment-tool



Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates

in Partnership with the  
National Learning Consortium

Newsroom | FAQs | Multimedia | Implementation Resources

Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Security Risk Assessment > Security Risk Assessment Tool

Print | Share

## Security Risk Assessment

Guide to Privacy and Security of Electronic Health Information

Health IT Privacy and Security Resources

Mobile Device Privacy and Security

Model Notices of Privacy Practices

Patient Consent for eHIE

Privacy & Security Training Games

Cybersecurity

Security Risk Assessment

Security Risk

### Security Risk Assessment Tool

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

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a

downloadable [SRA Tool \[exe - 69 MB\]](#) to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.



We understand that users with Windows 8.1 Operating Systems may experience difficulties downloading the SRA Tool, we are working to resolve the issue and will post here when a resolution is identified and implemented.

#### Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds.

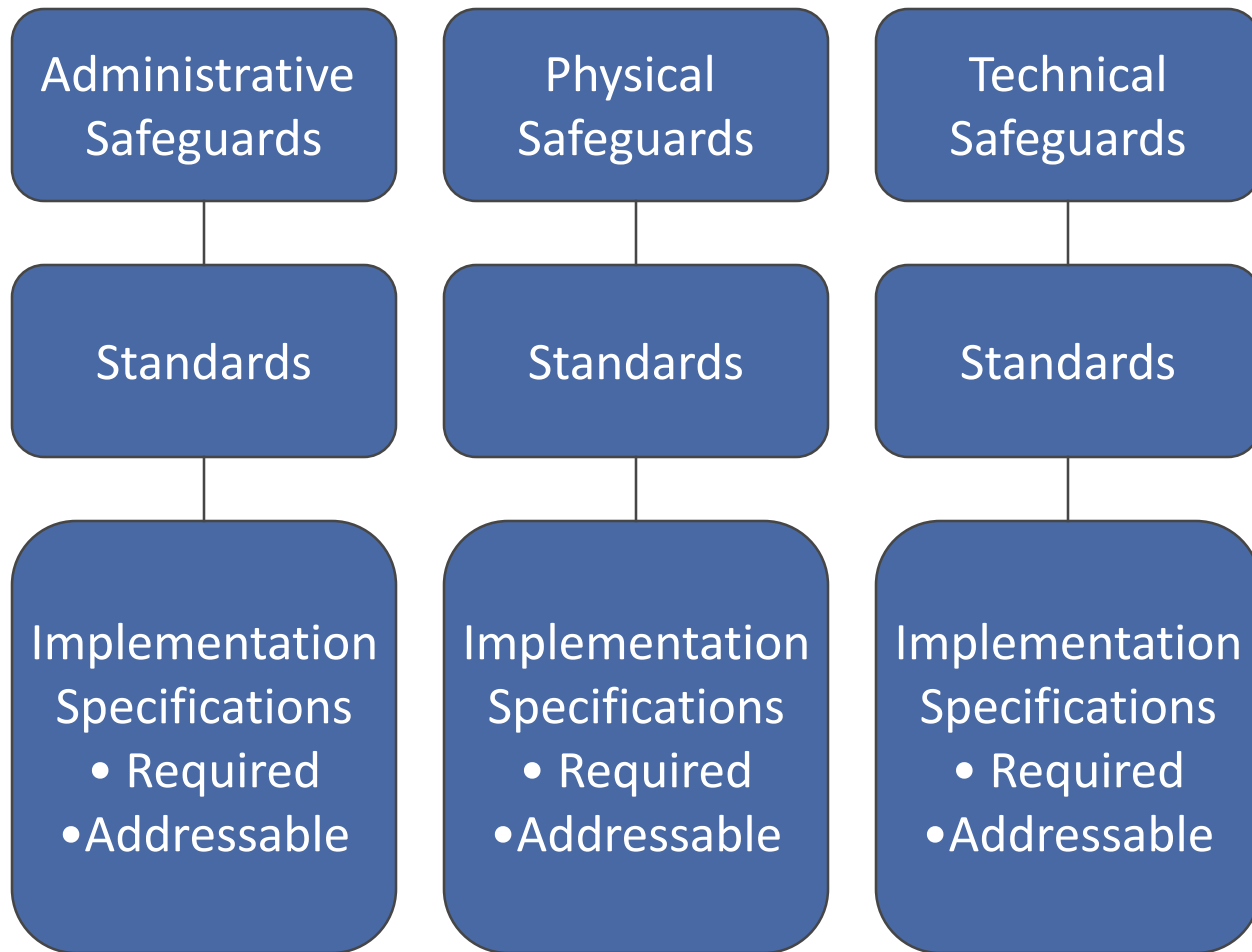
[Read the top 10 list distinguishing fact from fiction.](#)

#### SRA Tool (Windows version)



[Download Tool](#)

# SAFEGUARDS



I'm looking for...  [HHS A-Z Index](#)

 **HIPAA for Individuals**

 **Filing a Complaint**

 **HIPAA for Professionals**

 **Newsroom**

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

- HIPAA for Professionals
- Privacy
- Security 
  - Summary of the Security Rule
  - Guidance
  - Combined Text of All Rules
- Breach Notification
- Compliance & Enforcement
- Special Topics
- Patient Safety
- Covered Entities & Business Associates
- Training & Resources

Text Resize **A A A** Print  Share  

## Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).

[Security Risks to Electronic Health Information from Peer-to-Peer File Sharing Applications](#)-The Federal Trade Commission (FTC) has developed a guide to Peer-to-Peer (P2P) security issues for businesses that collect and store sensitive information.

[Safeguarding Electronic Protected Health Information on Digital Copiers](#)-The Federal Trade Commission (FTC) has tips on how to safeguard sensitive data stored on the hard drives of digital copiers.

## Security Rule Educational Paper Series

The HIPAA Security Information Series is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards.

[Security 101 for Covered Entities](#)

38  
[Administrative Safeguards](#)

[Physical Safeguards](#)

Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy and Security

Print | Share

# Privacy and Security

## Health Information Privacy, Security, and Your EHR

Ensuring privacy and security of health information, including information in electronic health records (EHR), is a key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.

Your practice, not your EHR vendor, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR and comply with The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules and CMS' Meaningful Use requirements.

Ensuring the Security of Electronic Health Records

0:00 / 2:34

YouTube



**Cybersecure:**

Your Medical Practice

[Play the Game](#)

### Integrating Privacy & Security Into Your Medical Practice

The HIPAA Privacy and Security Rules protect the privacy and security of health information.

### Privacy & Security 10 Step Plan

Ensuring privacy and security of health information in an EHR is a vital part of Meaningful Use. Security risk analysis and management are foundational to

### Privacy & Security and Meaningful Use

HIPAA privacy and security requirements are embedded in the Medicare and Medicaid EHR Incentive Programs through the following

# 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.



# BEWARE MOBILE DEVICES

providers-professionals/your-mobile-device-and-health-information-privacy-and-security



Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates



in Partnership with the  
National Learning Consortium

Newsroom | FAQs | Multimedia | Implementation Resources



Providers & Professionals

Patients & Families

Policy Researchers & Implementers

Benefits of EHRs

How to Implement EHRs

Privacy & Security

EHR Incentives & Certification

Success Stories & Case Studies

Resource Center

HealthIT.gov > For Providers & Professionals > Privacy & Security > Your Mobile Device and Health Information Privacy and Security

Print | Share

## Privacy & Security

### Your Mobile Device and Health Information Privacy and Security



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



#### Read and Learn

- How Can You Protect and Secure Health Information When Using a Mobile Device?
- You, Your Organization and Your Mobile Device
- Five Steps Organizations Can Take To Manage Mobile Devices



#### Watch and Learn

- Worried About Using a Mobile Device for Work? Here's What To Do!
- Securing Your Mobile Device is Important!
- Dr. Anderson's Office Identifies a Risk



# 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)

# PATIENT RIGHTS

- Notice of Privacy Practices
- Request restrictions on use or disclosure.
- Receive communications by alternative means.
- Access to info
- Amendment of info
- Accounting of disclosures of info

(45 CFR 164.520 et. seq.)

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

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

<b>HIPAA for Professionals</b>	
<b>Privacy</b>	-
Summary of the Privacy Rule	
Guidance	
Combined Text of All Rules	
<b>Security</b>	+

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

# ADMINISTRATIVE REQUIREMENTS

- Designate HIPAA privacy and security officers
- Implement policies and safeguards
- Train workforce
- Respond to complaints
- Mitigate violations
- Maintain documents for 6 years

(45 CFR 164.530)

# 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)

# “BREACH” OF UNSECURED PHI

- “Breach” defined to exclude the following:
  - 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 HIPAA privacy rule.
  - Inadvertent disclosure by authorized person to another authorized person at same covered entity, business associate, or organized health care arrangement, and PHI not further used or disclosed in violation of privacy rule.
  - Disclosure of PHI where covered entity or business associate have good faith belief that unauthorized person receiving info would not reasonably be able to retain info

(45 CFR 164.402)



# NOTICE TO INDIVIDUAL

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

(45 CFR 164.404(d))

# NOTICE TO HHS

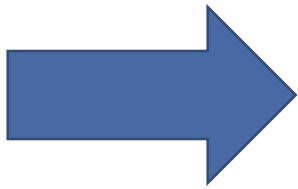
- If breach involves fewer than 500 persons:
  - Submit to HHS annually within 60 days after end of calendar year in which breach was discovered (i.e., by March 1).
- If breach involves 500 or more persons:
  - Notify HHS contemporaneously with notice to individual or next of kin, i.e., without unreasonable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

(45 CFR 164.408)

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

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

- HIPAA for Professionals
- Privacy +
- Security +
- Breach Notification -
  - Breach Reporting
  - Guidance
  - Reports to Congress
  - Regulation History
- Compliance & Enforcement +
- Special Topics +
- Patient Safety +
- Covered Entities & Business Associates
- Training & Resources
- FAQs for Professionals
- Other Administrative Simplification Rules



Text Resize A A A Print Share f t +

## Submitting Notice of a Breach to the Secretary

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

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

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

Please review the instructions below for submitting breach notifications.

### Breaches Affecting 500 or More Individuals

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

[Submit a Notice for a Breach Affecting 500 or More Individuals](#)

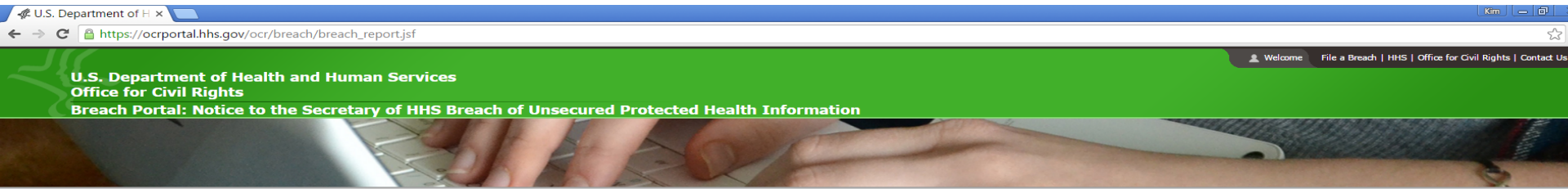
[View a list of Breaches Affecting 500 or More Individuals](#)

### Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which

# NOTICE TO HHS

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



## Breaches Affecting 500 or More Individuals

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. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results							
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information	
Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films	
Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server	
Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device	
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop	
Mark D. Lurie, MD	CA	Healthcare Provider	5166	11/20/2009	Theft	Desktop Computer	
L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer	
David I. Cohen, MD	CA	Healthcare Provider	857	11/20/2009	Theft	Desktop Computer	
Michele Del Vicario, MD	CA	Healthcare Provider	6145	11/20/2009	Theft	Desktop Computer	
Joseph F. Lopez, MD	CA	Healthcare Provider	952	11/20/2009	Theft	Desktop Computer	
City of Hope National Medical Center	CA	Healthcare Provider	5900	11/23/2009	Theft	Laptop	
The Children's Hospital of Philadelphia	PA	Healthcare Provider	943	11/24/2009	Theft	Laptop	
Cogent Healthcare, Inc.	TN	Business Associate	6400	11/25/2009	Theft	Laptop	
Democracy Data & Communications, LLC (	VA	Business Associate	83000	12/08/2009	Other	Paper/Films	
Kern Medical Center	CA	Healthcare Provider	596	12/10/2009	Theft	Other	
Rick Lawson, Professional Computer Services	NC	Business Associate	2000	12/11/2009	Theft	Desktop Computer, Electronic Medical Record, Network Server	
Detroit Department of Health and Wellness Promotion	MI	Healthcare Provider	646	12/15/2009	Theft	Desktop Computer, Laptop	
Detroit Department of Health and Wellness Promotion	MI	Healthcare Provider	10000	12/15/2009	Theft	Other Portable Electronic Device	

# 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)

# 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)

- Business associate agreements may impose different deadlines.

# IDAHO IDENTITY THEFT STATUTE

- Generally requires all 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 likely satisfies Idaho statute.

(IC 28-51-104)

# NEW DEVELOPMENTS

- Possible state and federal privacy laws
  - General Data Protection Regulation (EU)
  - California Consumer Privacy Act
  - Bipartisan support in Congress
- Proposed amendments to 42 CFR Part 2
  - Coordinates with HIPAA
  - Modifies disclosure rules for opioid cases
- FTC privacy enforcement
  - FTCA prohibits “unfair or deceptive trade practices”
  - “Unfair” = failure to protect data
  - “Deceptive” = failure to comply with privacy representations (e.g., notice of privacy practices)



# ADDITIONAL RESOURCES



# http://www.hhs.gov/hipaa/

HIPAA for Profession x

www.hhs.gov/hipaa/for-professionals/index.html

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...



HHS A-Z Index



HIPAA for Individuals



Filing a Complaint



HIPAA for Professionals



Newsroom

[HHS Home](#) > [HIPAA](#) > HIPAA for Professionals

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules

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



Share



## HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final [Privacy Rule](#) in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final [Security Rule](#) in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The [Enforcement Rule](#) provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a [final Omnibus rule](#) that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the [Breach Notification Rule](#).
- [View the Combined Regulation Text](#) (as of March 2013). This is an unofficial version that presents all the HIPAA regulatory standards in one document. The official version of all federal regulations is published in the Federal Register (FR) at [www.federalregister.gov](#).

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

Healthcare | Holland & H x

Secure | <https://www.hollandhart.com/healthcare#overview>

EXCELLENCE IN LEGAL SERVICE

MENU HOLLAND & HART 70 YEARS EST. 1947

OVERVIEW ▶

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS



**Kim Stanger**  
Partner  
Boise



**Blaine Benard**  
Partner  
Salt Lake City



**HEALTH LAW BLOG**  
Access to previous webinar recordings, publications, and more.

**The Healthcare Industry is now standing ready to help you**

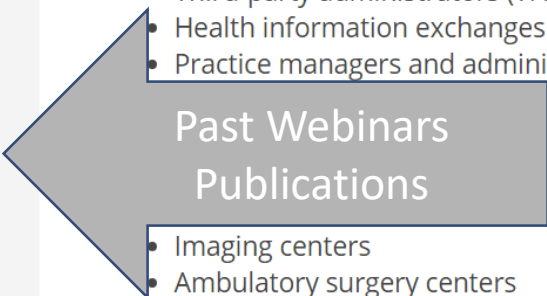
Issues such as rising health care costs, innovations in health care delivery, and the minds of many of our clients are creating new opportunities that arise from these changes.

**Clients We Serve**

- Hospitals
- Individual medical providers
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- Health information exchanges (HIEs)
- Practice managers and administrators
- Health care facilities

Past Webinars  
Publications

- Imaging centers
- Ambulatory surgery centers



# QUESTIONS?

Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

[kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com)

Lisa M. Carlson

Office: (208) 383-3910

Cell: (208) 949-0845

[lcarlson@hollandhart.com](mailto:lcarlson@hollandhart.com)