

# HIPAA Privacy: Common Problems & Compliant Solutions

**Kim C. Stanger**

**Compliance  
Bootcamp**

(5-17)



---

**This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.**

# Overview

---

- Why you should comply
  - Application: who, what, and whom
  - Use and disclosure rules
  - Authorizations v. patient requests
  - Business associates
  - Patient rights
  - Administrative requirements
  - Breach notification
  - “To Do” List
- We'll be moving fast



# Written Materials

---

- Copy of .ppt slides
- Checklists
  - HIPAA compliance
  - Required privacy policies and forms
  - Notice of privacy practices
  - Authorization
  - Business associate agreements
- OCR's recent guidance
  - Patient's Right to Access Information
  - HIPAA and Cloud Computing
- Available at <http://www.hhhealthlawblog.com/>

# 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



Privacy Protection

**More  
restrictive law**

**HIPAA**

**Less restrictive  
law**

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



# HIPAA Enforcement



# 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>

(42 USC 1320d-6(a))



# Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none"><li>• \$100 to \$50,000 per violation</li><li>• Up to \$1.5 million 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>• \$1000 to \$50,000 per violation</li><li>• Up to \$1.5 million 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>
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none"><li>• \$10,000 to \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none"><li>• At least \$50,000 per violation</li><li>• Up to \$1.5 million per type per year</li><li>• <b>Penalty is mandatory</b></li></ul>

(45 CFR 160.404)

# HIPAA Settlements this Year

Conduct	Settlement
Hospital issued press release containing patient's name after patient used fraudulent identification card.	\$2,400,000
Monitoring company's laptop containing 1,390 patients' info stolen from car; <b>insufficient risk analysis and no finalized security policies.</b>	\$2,500,000
<b>No business associate agreement ("BAA")</b> with record storage company.	\$31,000
FQHC's info hacked; <b>no risk analysis and insufficient security rule safeguards.</b>	\$400,000
Hospital allowed unauthorized employees to access and disclose records of 80,000 patients; failed to terminate users' right of access.	\$5,500,000
Hospital <b>lost unencrypted PDAs</b> containing info of 6,200 persons; failure to take timely action to address known risks.	\$3,200,000
Insurance company's <b>unencrypted USB</b> containing info of 2,209 persons stolen; no risk analysis, implementation, or encryption.	\$2,200,000
<b>Failure to timely report breach.</b>	\$475,000

## Small hospice in Idaho pays \$50,000

- Stolen laptop containing 441 patients' info
- No risk analysis.
- No policies for mobile device security.

**“This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information.”**

**FOR IMMEDIATE RELEASE**  
**January 2, 2013**

**Contact: HHS Press Office**  
**202-690-6343**  
[media@hhs.gov](mailto:media@hhs.gov)

## HHS announces first HIPAA breach settlement involving less than 500 patients

*Hospice of North Idaho settles HIPAA security case for \$50,000*

The Hospice of North Idaho (HONI) has agreed to pay the U.S. Department of Health and Human Services' (HHS) \$50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. This is the first settlement involving a breach of unsecured electronic protected health information (ePHI) affecting fewer than 500 individuals.

The HHS Office for Civil Rights (OCR) began its investigation after HONI reported to HHS that an unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients had been stolen in June 2010. Laptops containing ePHI are regularly used by the organization as part of their field work. Over the course of the investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI. Further, HONI did not have in place policies or procedures to address mobile device security as required by the HIPAA Security Rule. Since the June 2010 theft, HONI has taken extensive additional steps to improve their HIPAA Privacy and Security compliance program.

“This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information.” said OCR Director Leon Rodriguez. “Encryption is an easy method for making lost information unusable, unreadable and undecipherable.”

The Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a “breach,” of 500 individuals or more to the Secretary of HHS and the media within 60 days after the discovery of the breach. Smaller breaches affecting less than 500 individuals must be reported to the Secretary on an annual basis.

*A new educational initiative: Mobile Devices: Know the DISKS, Take the STEPS, DDOTECT and*

# 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.
- OCR is conducting Phase 2 audits.
- 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.
  - State tort claims
  - State privacy laws
  - Consumer protection statutes
  - FTCA
  - FCRA

# Covered Entities and Info

---



# 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

- Unauthorized disclosure outside covered entity.
- Unauthorized use within covered entity.
- Unauthorized access from within or outside covered entity.



IFL4QEQHEP.COM



# 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 discuss 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)

# Other Law Requires Disclosure

---

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

(45 CFR 164.512(a))



# Disclosures Required by Law

---

- **Child abuse or neglect. (IC 16-1605; see also 45 CFR 164.512(b))**
- **Vulnerable adult abuse or neglect. (IC 39-4503; 45 CFR 164.512(c))**
  - **Must notify vulnerable adult. (45 CFR 164.512(c))**
- **Treatment of victim of crime or injury by firearm. (IC 39-1390)**
- **Patient made explicit threat of imminent serious physical harm or death to clearly identified or identifiable victim, and patient has apparent intent and ability to carry out such a threat. (IC 6-1901 et seq.)**
- **Custody of body if death occurred from violence, under suspicious or unknown circumstances, or is of a child if there is reasonable suspicion to believe death occurred without a known medical disease to account for the death. (IC 19-4301A)**

# Disclosures Required by Law

---

- **Blood tests which confirm the presence of blood-transmitted or bodily fluid-transmitted virus or disease (IC 39-4505).**
- **Certain reportable infectious, contagious, or communicable diseases. (IC 39-602; IDAPA 16.02.10.20)**
- **Births, deaths, stillborns, and induced abortions (IC 39-255, -260, -261, and -272).**
- **Inflammation of eyes of newborn (IC 39-902)**
- **Results of PKU tests (IC 39-909)**
- **Don't forget about local laws or ordinances...**

*(See also 45 CFR 164.512(b))*

# Serious and Imminent Harm

---

- **May use or disclose PHI to if believe in good faith 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.
    - See recent guidance at <https://www.hhs.gov/hipaa/newsroom/patient-safety-work-product-guidance-news/index.html>
  - 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.



(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))



# Workers Comp

---

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

(45 CFR 164.512(I))

- **In Idaho:**
  - **Must disclose info relevant to occupational injury or disease to employer, surety, manager, fund, or their attorney. (IC 72-432)**
  - **Must disclose written medical reports to claimant upon request and at no charge. (IDAPA 17.02.04.322)**

# 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))

# Patient Authorizes Disclosure

- Written requests
- Authorizations



# Patient Request to Provide Information

---

- **Must provide 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 may not be combined with other documents.**
- **Authorization must contain required elements and statements.**

(45 CFR 164.508)

# Authorization

---

- **Required Elements**
  - Written in plain language.
  - Describe PHI to be disclosed.
  - Identify entity authorized to make disclosure.
  - Identify entity to whom disclosure made.
  - Describe purpose of disclosure.
    - “At request of individual” if patient initiates.
  - Include expiration date or event.
  - Dated and signed by patient or representative.
  - State authority of personal representative.

(45 CFR 164.508)

# Authorization

---

- **Required Statements**
  - Right to revoke the authorization in writing at anytime and either:
    - Describe exceptions and how to revoke, or
    - Refer to Notice of Privacy Practices where such info may be found.
  - Cannot condition treatment or payment on authorization.
  - PHI may be re-disclosed and, if so, may not be protected.

(45 CFR 164.508)

# Psychotherapy Notes

- **Must have authorization to use or disclose psych notes except for provider's use of own notes for treatment purposes.**
  - “Psych notes” are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.
  - “Psych notes” excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- **Psych authorization cannot be combined with any other authorization.**

(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))

# Marketing

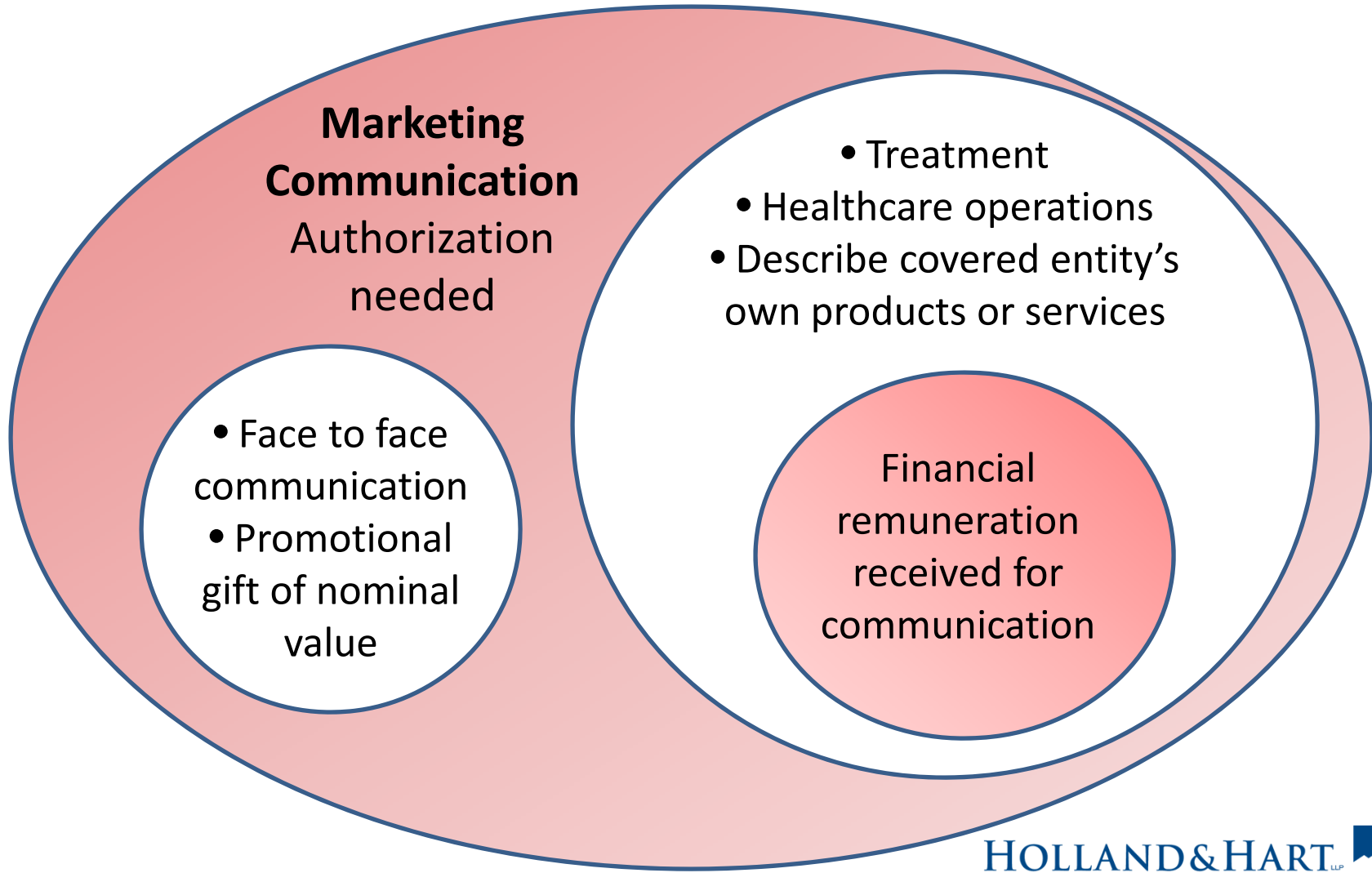
- If covered entity receives financial remuneration from third party in exchange for making communication about the third party's items or services, then the following are "marketing" and covered entity must obtain patient's authorization to use or disclose PHI to market:
  - provide refill reminders or communicate about drug currently being prescribed unless remuneration is related to cost of making the communication.
  - for treatment purposes, including case management, care coordination, or recommendations for treatment alternatives, providers, etc.
- Authorization must disclose that covered entity is receiving remuneration.

# Marketing

---

- Even though covered entity receives financial remuneration, authorization is not required if:
  - communication is for treatment, healthcare operations or other marketing occurs in face-to-face communication with patient, or
  - consists of promotional gift of nominal value provided by the covered entity.
- Authorization would be required for such communications via telephone or e-mail since they are not “face-to-face”.

**Marketing = communication about product or service that encourages recipient to purchase or use product or service .**



# 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)

# Sale of PHI

---

- **Does not apply to disclosures:**
  - for treatment or payment purposes.
  - as part of sale of covered entity.
  - to business associate and payment is for business associate's duties.
  - for purposes allowed by HIPAA and payment is reasonable cost-based fee to transmit PHI.
  - Recovery of fees allowed by law.
- **Per commentary, does not apply to:**
  - payments to provide services or grants.
  - payments to participate in health information exchange.

# 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/](http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/)

(164.512(i) and elsewhere)

# To summarize use and disclosure rules

---

- **Cannot use or disclose PHI unless—**
  - For purposes of treatment, payment, or healthcare operations.
  - For disclosures to family members and others involved in patients care or payment for care if
    - Patient has not objected,
    - Disclosure appropriate under circumstances, and
    - Limit disclosure to person’s involvement.
  - For certain safety or government purposes as listed in 45 CFR 164.512.
  - Have a valid written authorization or request signed by patient that complies with 45 CFR 164.508 or 164.524.

# 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))

- 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

---

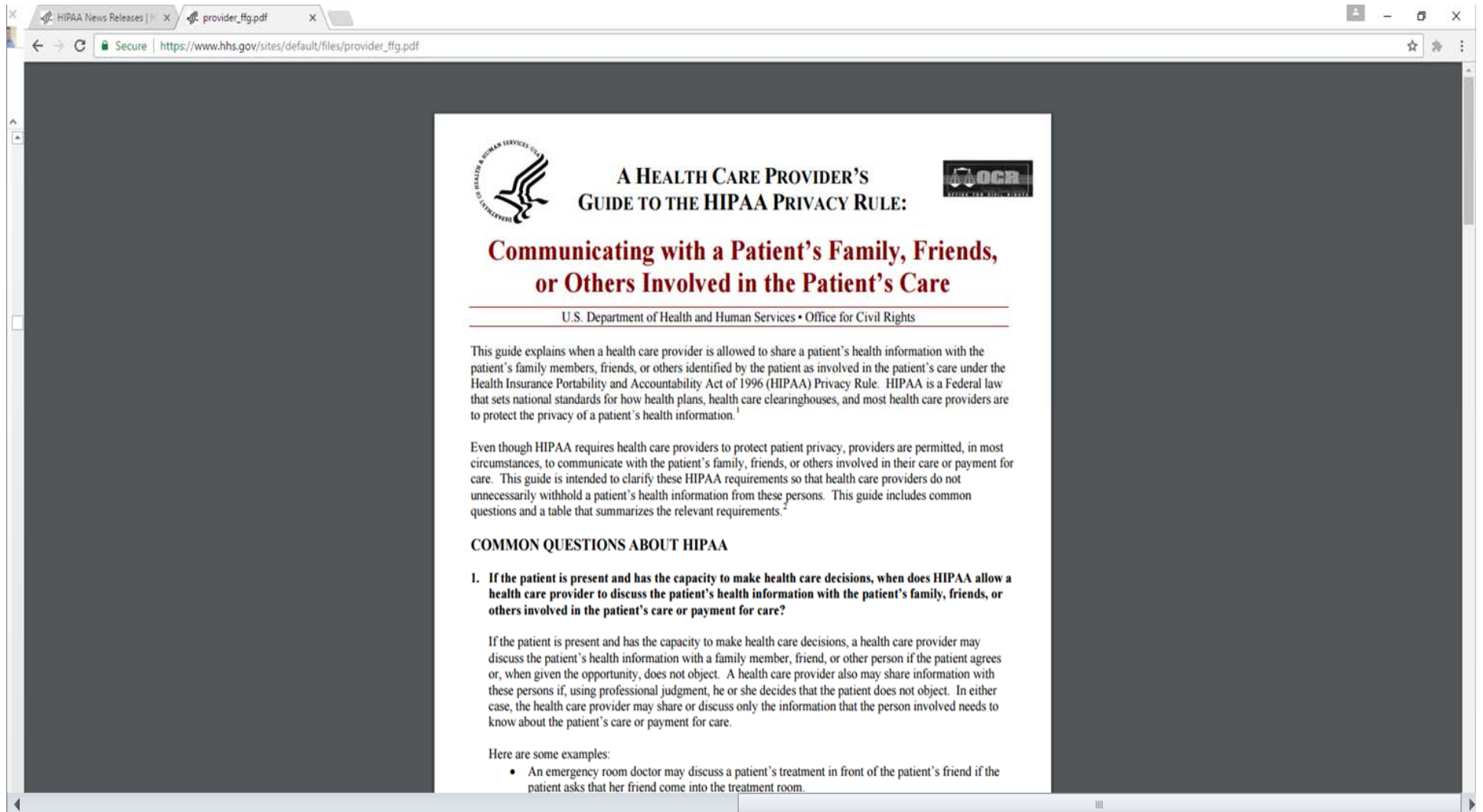
- **Not required to treat personal rep as patient (i.e., do not disclose PHI to them) if:**
  - **Minor has authority to consent to care.**
  - **Minor obtains care at the direction of a court or person appointed by the court.**
  - **Parent agrees that provider may have a confidential relationship.**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

# Summary: Family Members and Personal Representatives

---

- **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](http://www.hhs.gov/ocr/privacy/hipaa), available at [www.hhs.gov/ocr/privacy/hipaa](http://www.hhs.gov/ocr/privacy/hipaa).*

[https://www.hhs.gov/sites/default/files/provider\\_ffg.pdf](https://www.hhs.gov/sites/default/files/provider_ffg.pdf)



The image shows a browser window displaying a PDF document. The browser's address bar shows the URL: [https://www.hhs.gov/sites/default/files/provider\\_ffg.pdf](https://www.hhs.gov/sites/default/files/provider_ffg.pdf). The document content includes the following elements:

- Logos:** The U.S. Department of Health and Human Services (HHS) logo on the left and the Office for Civil Rights (OCR) logo on the right.
- Title:** "A HEALTH CARE PROVIDER'S GUIDE TO THE HIPAA PRIVACY RULE:"
- Section Header:** "Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care"
- Author:** "U.S. Department of Health and Human Services • Office for Civil Rights"
- Text:**

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>
- Section Header:** "COMMON QUESTIONS ABOUT HIPAA"
- Question 1:** "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?"
- Text:**

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.
- Text:**

Here are some examples:
- List-Group:**
  - 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



# 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

- Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity to perform:
  - A function or activity regulated by HIPAA (e.g., healthcare operations, payment, covered entity function), or
  - Certain identified services (e.g., billing or claims management, legal, accounting, or consulting services).
  - Health information organizations and e-prescribing gateways.
  - Data transmission companies if they routinely access PHI.
  - Data storage companies (e.g., cloud computing, off-site storage facilities) even if they do not access PHI or data is encrypted.
  - Patient safety organizations.
- Covered entities acting as business associates.
- Subcontractors of business associates.

(45 CFR 160.103)

# 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 Article, Avoiding BAAs*

# Business Associate Decision Tree

Will an outside entity ("Entity") provide services to or on behalf of the covered entity?

[Note: This does not apply to (1) an employee, volunteer, trainee, or other person whose conduct is under the direct control of the covered entity, (2) an entity who is performing functions as part of the covered entity's organized health care arrangement,<sup>1</sup> or (3) entities who receive info for their own purposes, and not to provide services to or on behalf of the covered entity (e.g., payors, government agencies, independent researchers, etc.).]

No  
The Entity is not a business associate

Yes

Will the Entity create, receive, maintain or transmit PHI in the course of providing services to or on behalf of the covered entity?

[Note: This does not apply to entities who may incidentally see or hear PHI, but whose job duties for the covered entity do not involve the creation, receipt, maintenance, or transmission of PHI (e.g., a janitor, delivery person, or electrician who happens to be providing services in the building)].

No  
The Entity is not a business associate

Yes

Is the Entity a healthcare provider who is receiving the PHI for purposes of treating the individual?

Yes  
The Entity is not a business associate

No

Does the Entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity?  
OR  
Does the Entity provide claims processing or administration; data analysis, processing or administration; or utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing services for the covered entity?  
OR  
Is the Entity a health information organization, e-prescribing gateway, or other entity that provides data transmission services with respect to PHI and the entity requires access to the PHI on a routine access (i.e., the entity is not merely the conduit for the information)?  
OR  
Does the Entity offer a personal health record to one or more individuals on behalf of the covered entity?

No  
The Entity is not a business associate

Yes

The Entity is a business associate. You must execute a valid business associate agreement with the Entity before disclosing PHI to the Entity. The business associate agreement must contain the elements in 45 CFR §§ 164.314(a) and 164.504(e)

<https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>

The screenshot shows a web browser window displaying the HHS.gov website. The address bar shows the URL: <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>. The page header includes the HHS.gov logo and the text "U.S. Department of Health & Human Services" and "Health Information Privacy". A search bar with the placeholder text "I'm looking for..." is visible. Below the search bar are four navigation buttons: "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". The breadcrumb trail reads: [HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Special Topics](#) > Cloud Computing. The page content includes a "Text Resize" tool (AAA), a "Print" button, and "Share" options for Facebook, Twitter, and a plus sign. The main heading is "Guidance on HIPAA & Cloud Computing". Below the heading is an "Introduction" section with the following text: "With the proliferation and widespread adoption of cloud computing solutions, HIPAA covered entities and business associates are questioning whether and how they can take advantage of cloud computing while complying with regulations protecting the privacy and security of electronic protected health information (ePHI). This guidance assists such entities, including cloud services providers (CSPs), in understanding their HIPAA obligations." A sidebar on the left contains expandable sections: "HIPAA for Professionals", "Privacy", "Security", "Breach Notification", and "Compliance & Enforcement". The Windows taskbar at the bottom shows the time as 10:04 PM on 2/13/2017.

# Cloud Services Providers

- **CSPs are BAs if they store PHI even though:**
  - They do not access data.
  - Data is encrypted and CSP does not have access key.
    - Must still ensure the availability and integrity as well as confidentiality of the e-PHI.
- **Must have BAA with CSP.**
  - Oregon Health & Science University paid \$2,700,00.
- **CSP not liable if it did not know CE was using CSP to create, receive, maintain or transmit PHI.**
  - Upon learning of such acts, CSP must correct situation within 30 days.

# Business Associate Agreements ("BAA")

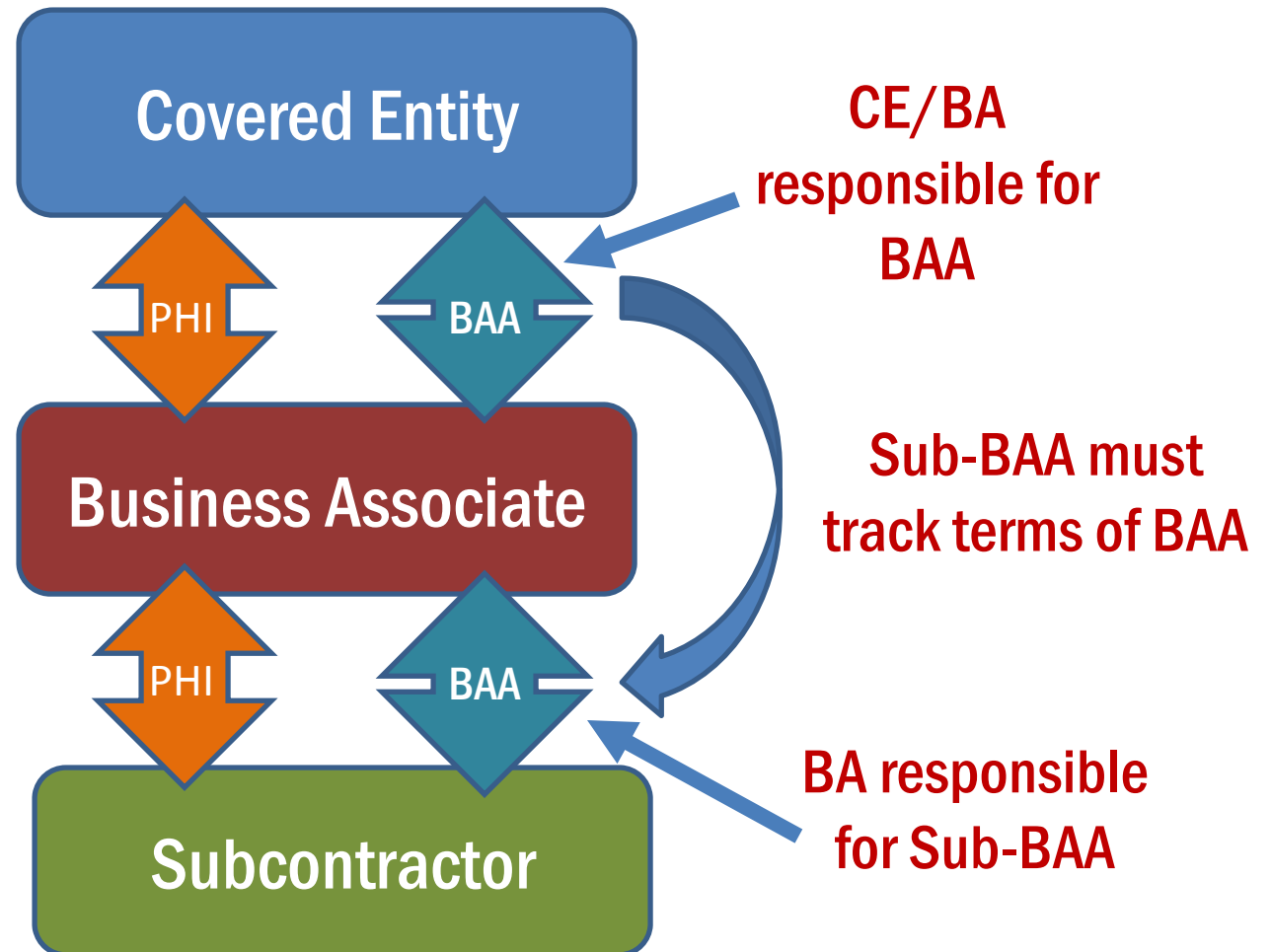




# BAA

- **Covered entity must have BAA before disclosing PHI to business associate or authorizing business associate to create or receive PHI for covered entity.**
  - BAA limits business associate's use of PHI.
- **Business associate must have BAA with subcontractor.**
  - Must match scope of BAA between covered entity and business associate.
- **Must comply with terms of BAA.**
  - Breach of contract with covered entity.
  - HIPAA penalties imposed by OCR.
- **Must comply with HIPAA even if no BAA.**

# Business Associates



# BAA: Required Terms

---

- **Establish permitted uses of PHI.**
  - **Business associate may only use or disclose PHI:**
    - As allowed by BAA, or
    - As required by law.
  - **May allow business associate to use for its internal management or administration.**
  - **Business associate may not use or disclose PHI in a manner that would violate the Privacy Rule if done by covered entity.**
    - Beware situations where covered entity has limited use or disclosure through, e.g., Notice of Privacy Practices or agreement.

# BAA: Required Terms

---

- **Implement safeguards to protect PHI.**
  - Privacy Rule safeguards are not specified.
- **Comply with HIPAA Security Rule.**
  - Perform and document a risk assessment.
  - Implement administrative, technical and physical safeguards.
  - Execute subcontractor BAAs.
  - Maintain written policies and documentation.
  - Train personnel.

# BAA: Required Terms

---

- **Report to covered entity:**
  - **Breaches of unsecured PHI.**
    - Per breach reporting rules.
  - **Use or disclosure of PHI not allowed by BAA.**
    - HIPAA violations even if not reportable breach.
    - BAA violations even if doesn't violate HIPAA.
  - **“Security incidents”, i.e., attempted or successful unauthorized access, use, disclosure, modification, or destruction of info or interference with system operations.**
    - BAA may allow business associate to give periodic notice of unsuccessful “security incidents”. (OCR Guidance on HIPAA & Cloud Computing)

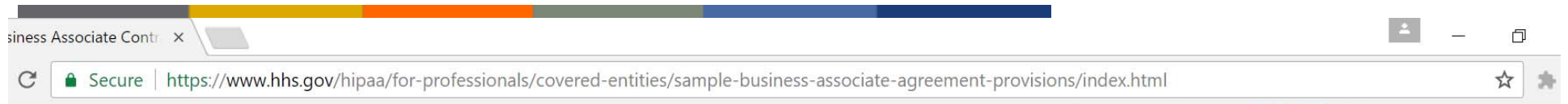
# BAA: Required Terms

- Cooperate in providing individuals with access to PHI in designated record set.
- Cooperate in amending records in designated record set.
- Cooperate in providing accounting of disclosures of PHI in designated record set.
  - Must log improper disclosures and certain disclosures for public safety or government functions, including:
    - Date of disclosure;
    - Name of entity receiving disclosure;
    - Description of info disclosed; and
    - Describe purpose of disclosure.

# BAA: Required Terms

- If covered entity delegates its functions to business associate, comply with HIPAA as to those functions.
- Make internal records available to HHS for inspection.
- Execute BAAs with subcontractors.
  - Must parallel BAA with covered entity.
- Authorize termination if business associate violates terms.
- Upon termination of BAA:
  - Return or destroy all PHI if feasible.
  - If not feasible to return or destroy PHI, comply with BAA as to any PHI it retains.

# <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





# BAA: Pro-Covered Entity Terms

- Covered entities may want to add these terms:
  - Business associate must report or act within x days.
  - Business associate must implement policies.
  - Business associate must encrypt or implement other safeguards.
  - Business associate must carry data breach insurance.
  - Business associate notifies individuals of breaches and/or reimburses covered entity for costs of the notice.
  - Business associate defends and indemnifies for losses, claims, etc.
  - Business associate is an independent contractor, not agent.
  - Business associate assumes liability for subcontractors.
  - Allow termination of underlying agreement.
  - Must have consent to operate outside the United States.
  - Covered entity has right to inspect and audit.
  - Cooperate in HIPAA investigations or actions.
  - Business associate not excluded from Medicare.
- \* *Business associate may want these in subcontracts.*

# BAA: Pro-BA Terms

- **Business associates and subs probably want to add these:**
  - Condition obligations on status as business associate.
  - Covered entity will not disclose PHI unless necessary.
  - Covered entity will not request action that violates HIPAA.
  - Covered entity has obtained necessary authorizations.
  - Covered entity will not agree to restrictions on PHI that will adversely affect BA.
  - Covered entity will notify business associate of all such restrictions.
  - Covered entity will reimburse for additional costs.
  - Blanket reporting for security incidents.
  - Specify business associate does not maintain designated record set.
  - Reserve the right to terminate based on restrictions or other change that adversely affects business associate.
  - Subcontractors are independent contractors, not agents.
  - Mutual indemnification.
  - Limitation or cap on damages.

# BAA Negotiation

It comes down to bargaining power...



# Liability for Acts of Business Associate or Subs

- CE or BA is liable, in accordance with the Federal common law of agency, for the acts or omissions of a BA/sub-BA acting with the scope of the agency.

(45 CFR 160.402(c)).

- Test: right or authority of a CE covered entity to control the BA's 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)

# Liability for Acts of Business Associate or Subs

---

- Covered entity or business associate violates HIPAA if:
  - Knew of a pattern of activity or practice of the business associate/subcontractor that constituted a material breach or violation of the business associate's/subcontractor's obligation under the contract or other arrangement;
  - Failed to take reasonable steps to cure the breach or end the violation, as applicable; or
  - Failed to terminate the contract or arrangement, if feasible.

(45 CFR 164.504(e)(1))

- Maybe if failed to execute BAA.
  - See recent settlements.

# No Duty to Monitor BA

- “[HIPAA] does not require a covered entity to actively monitor the actions of its business associates .... Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate’s obligations under the contract, the covered entity take steps to cure the breach or end the violation. See § 164.504(e)(1).”

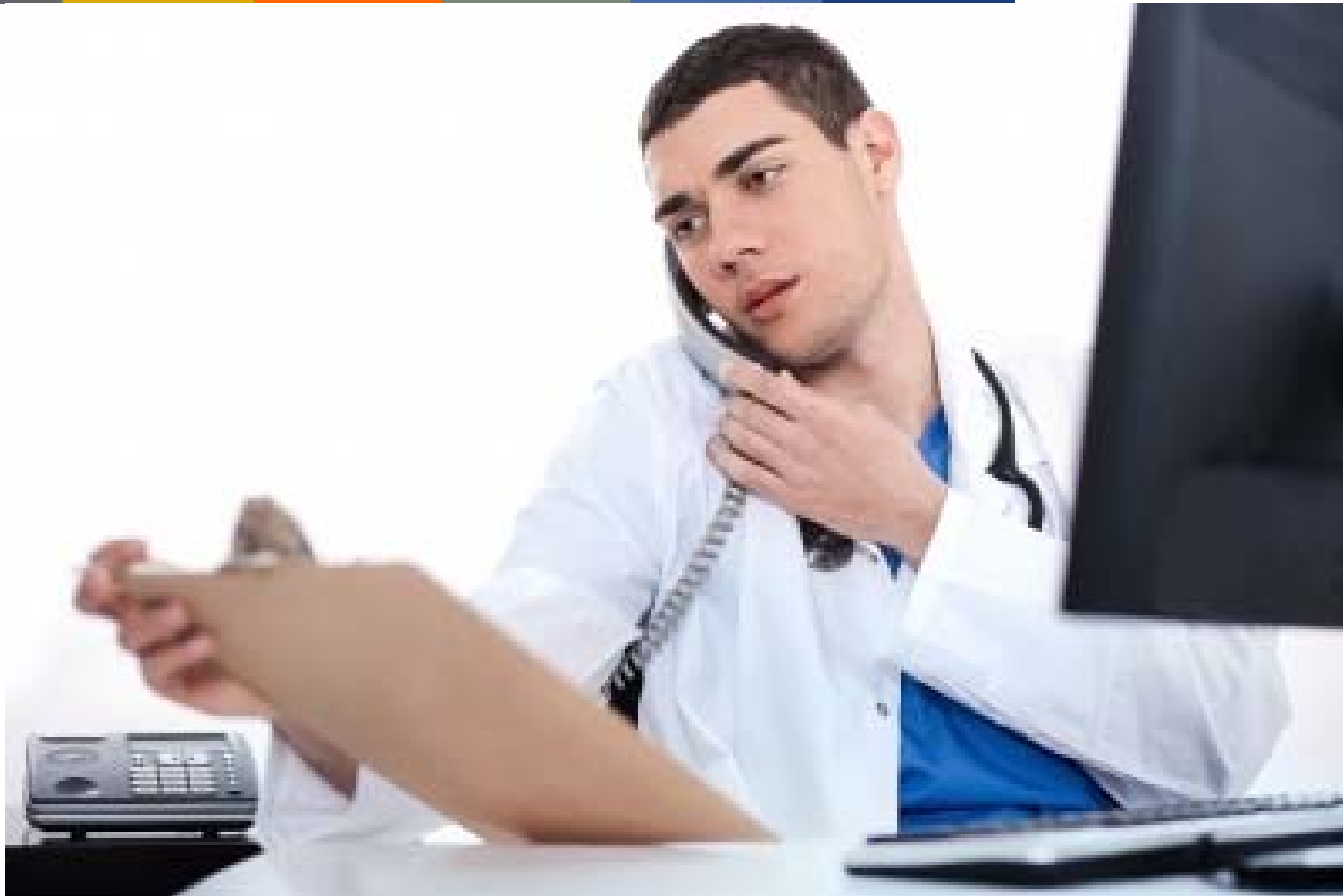
(67 FR 53252; *see also* FAQ available at <https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html>).

# BAA: Summary

---

- **CEs: when in doubt, demand BAA.**
- **BAs: do not assume BAA liability unless you must.**
- **Review terms of BAA carefully.**
  - Beware terms that are not required by HIPAA.
  - Beware terms that increase liability.
- **Remember: if you are a BA, you must comply with HIPAA requirements whether or not you have a BAA.**
- **Ensure you comply with BAA terms.**
  - Ensure your workforce understands requirements.
  - You likely must report disclosures in violation of BAA.
  - Disclosures in violation of BAA are HIPAA violations.

# Making the Disclosure





# Disclosure Optional

- Privacy rules usually allow you to make disclosures, but do not require it.
  - May decline to make disclosure even though privacy laws would let you make disclosure.
- Exceptions: must disclose—
  - To patient or authorized personal representative.
  - Per court order or warrant.
  - As required by other laws.

(45 CFR 164.502)

# 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.

# Patient Rights



# Notice of Privacy Practices

---

- **Notice summarizes HIPAA rules and explains how you will use the patient's information.**
  - **Must contain certain provisions.**
- **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)

# [www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html)





Model Notices of Privacy x

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





**HHS.gov** U.S. Department of Health & Human Services  
**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](#) > Model Notices of Privacy Practices

Text Resize **A A A** Print  Share   

**HIPAA for Professionals**

**Privacy** 

- [Summary of the Privacy Rule](#)
- [Guidance](#)

## Model Notices of Privacy Practices

The HIPAA Privacy Rule requires health plans and covered health care providers to develop and distribute a notice that provides a clear, user friendly explanation of individuals rights with respect to their personal health information and the privacy practices of health plans and health care providers. This page provides options for meeting the requirement to create notices of privacy practices (NPP).

HHS developed the model NPPs you see on this site to help improve patient experience and understanding. These models use plain language and approachable designs.

# 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 request of a patient 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.
- **Don't ask the patient!**  
(45 CFR 164.522)

# 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 employees or providers.**

# Right to Access Information


- 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](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)

Individuals' Right under HIPAA to Access their Health Information

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


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

# Right to Access Information

---

- May require request in writing if inform individual.
- Must verify identity and authority if requester not known.
- May not create barrier or unreasonably delay access, e.g., may not:
  - require patient to come to physician's office to pick it up.
  - use web portal to request access.
  - mail access request.

# Right to Access Information

- If covered entity accepts the request:
  - Must provide records in form requested if readily producible, e.g.,
    - Paper
    - Electronic
  - May provide summary if individual agrees.
  - Must produce records at time and in manner that is reasonably convenient.
    - Mail and e-mail are presumptively reasonable.
    - May not require patient to physically pick up records.

# Right to Access Information

- **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.
- **May charge flat fee of \$6.50 per request for electronic records.**
- **Cannot charge for CEHRT (view, download, transmit function)**

(OCR Clarification of Permissible Fees)



# Right to Access Information

---

- Patient has right to direct that info 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.
- Limits applicable to patient apply to such requests.
  - Must respond within 30 days.
  - Must provide in form and format requested.
  - May only charge a reasonable cost-based fee.
- Must take reasonable steps to protect the PHI in transit.

# Right to Access Information

---

- 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.

# 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 all disclosures made for prior 6 years.
  - Improper disclosures
    - Different than breach notification.
  - Disclosures made per 164.512, e.g., disclosures
    - Required by law.
    - For public health activities.
    - For health oversight activities.
    - For certain law enforcement purposes.
- Must respond to request within 60 days.
  - May obtain 30-day extension.

(45 CFR 164.528)

# Right to Accounting of Disclosures

---

- Accounting must include:
  - Date of disclosure.
  - Name of entity receiving disclosure.
  - Description of info disclosed.
  - Describe purpose of disclosure.
- Must keep track of this information so that you can provide accounting.
- Must account for disclosures made by business associates.
- Must account for disclosure even if you are not required to report it under breach notification rules.

# Right to Accounting of Disclosures

- HITECH Act requires HHS to issue regulations allowing individuals to obtain an accounting of disclosures made for purposes of treatment, payment and healthcare operations if the disclosure is through an electronic health record.

(HITECH Act 13405)

- HHS issued a proposed rule that would entitle individuals to obtain a broad report concerning those who accessed their PHI or to whom their PHI was disclosed.

(76 FR 31426 (5/31/11))

- Subject to future rulemaking.

(78 FR 5568)

*\* Watch for new rule.*

# Administrative Requirements



# Designate Officials

---

- **Must designate HIPAA officers in writing:**
  - Privacy officer: privacy policies
  - Security officer: security rules
  - Contact person: questions and complaints
  - Document appointment
- **May be same person.**

(45 CFR 164.530(a))



# Implement Policies

---

- **Implement written policies to ensure compliance with rules.**
  - Modify to match changes in law
  - Coordinate notice of privacy practices
- **Consider using valid forms.**
  - Authorization
  - Notice of privacy practices
  - Business associate agreement
  - Request to access info
  - Request to amend info

# Train Workforce

---

- **Train workforce, i.e., those over whom you have control, e.g., employees, volunteers, students, temps.**
  - New members: within reasonable time.
  - Changes in law or policy: within reasonable time.
- **Document training.**

(45 CFR 164.530(b))

# Reasonable Safeguards

- Implement administrative, physical and technical safeguards to limit improper intentional or inadvertent disclosures.
  - No liability for “incidental disclosures” if implemented reasonable safeguards.
  - Problem: what is “reasonable”?
    - Protections are “scalable” and should not interfere with health care
    - See OCR Guidance at [www.hhs.gov/ocr/hipaa/privacy](http://www.hhs.gov/ocr/hipaa/privacy)

(45 CFR 164.530(c))

# Reasonable Safeguards per OCR Guidance

---

## **NOT** required to:

- Remodel.
- Eliminate sign-in sheets.
- Isolate x-ray boards.
- Remove bedside charts.
- Buy a computer.

## **MAY** be required to:

- Keep records, monitors, faxes from view of unauthorized persons.
- Minimize eavesdropping.
- Supervise or lock areas where records stored.
- Use passwords.
- Avoid patient names in public.

# Respond to Complaints and Violations

---

- Provide process for handling and documenting patient complaints.
- Impose and document sanctions against workforce members who violate policies.
- Mitigate wrongful use or disclosures.
- Do not retaliate.
- Do not require waiver of HIPAA rights.
- Document response.

(45 CFR 164.530(d)-(g))

# Maintain Documentation

- **Maintain required documentation required by HIPAA for 6 years, e.g.,**
  - Privacy notices and acknowledgments.
  - Policies.
  - Personnel designations.
  - Patient requests and denials.
  - Accountings.
  - Employee training.
  - Complaints.
  - Sanctions.
  - Communications that are required to be in writing.
  - Activities that are required to be documented.

(45 CFR 164.530(j))

# Breach Reporting (45 CFR 164.400)

---



# 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.)



# “Secured” PHI

Currently, only two methods to secure PHI:

- **Encryption of electronic PHI**
  - Transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
  - Notice provides processes tested and approved by Nat’l Institute of Standards and Technology (NIST).
- **Destruction of PHI.**
  - Paper, film, or hard copy media is shredded or destroyed such that PHI cannot be read or reconstructed.
  - Electronic media is cleared, purged or destroyed consistent with NIST standards.

(74 FR 42742 or [www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy))

# “Breach” of Unsecured PHI

- Acquisition, access, use or disclosure of PHI in violation of privacy rules 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)

# “Breach”: Risk Assessment

- Determine the probability that the data has been “compromised” by assessing:
  1. Nature and extent of PHI involved, including types of identifiers and the likelihood of re-identification.
  2. Unauthorized person who used PHI or to whom disclosure was made.
  3. Whether PHI was actually acquired or viewed.
  4. Extent to which the risk to the PHI has been mitigated.
  5. Other factors as appropriate under the circumstances.

(45 CFR 164.402)

- Risk assessment is unnecessary if make report.

# “Breach”: Risk Assessment

- Based on commentary, following situations likely involve lower probability that PHI would be compromised.
  - Fax sent to wrong physician, but physician reports fax and confirms he has destroyed it.
  - Disclosure to or use by persons who are required by HIPAA to maintain confidentiality.
  - Disclosure without identifiers or to entity that lacks ability to re-identify the PHI.
  - Stolen laptop recovered and analysis shows that PHI was not accessed.
- But must evaluate all factors.

(78 FR 5642-43)

# “Breach”: Risk Assessment

- Based on commentary, following situations likely involve higher probability that PHI is compromised.
  - Disclosure involves financial data (e.g., credit card numbers, SSN, etc.), sensitive info (e.g., STDs, mental health, or other info), or detailed info (e.g., treatment plan, diagnosis, medication, medical history, test results).
  - Disclosure involves list of patient names, addresses, hospital IDs.
  - info mailed to wrong individual who opened and read it; person is not a covered entity or business associate.
- But must evaluate all factors.
- HHS will issue future guidance regarding common scenarios.

(78 FR 5642-43)

# Breach of Unsecured PHI: Summary

---

- **No breach notification required if:**
  - No privacy rule violation.
    - “Incidental disclosures” do not violate the privacy rule.
  - PHI is “secured”, i.e., encrypted per HHS standards.
  - Exception applies, i.e.,
    - Unintentional acquisition of PHI by workforce member acting in good faith and no further use or redisclosure.
    - Inadvertent disclosure by authorized person to another person authorized to access the PHI.
    - Unauthorized recipient of PHI is unable to retain PHI.
  - Low probability that data has been compromised.
- **Covered entity has burden of proof.**

# Breach of Unsecured PHI: Summary

---

- **Until we receive further clarification, safer to err on the side of reporting all but clearly “inconsequential” breaches.**
  - **Covered entity has burden of proving “low probability that PHI has been compromised.”**
  - **Failure to report may be viewed as willful neglect resulting in mandatory penalties.**



# Breach of Unsecured PHI: Summary

---

- According to HHS, the following constitutes “willful neglect”, requiring mandatory penalties:

“A covered entity’s employee lost an unencrypted laptop that contained unsecured PHI.... [T]he covered entity feared its reputation would be harmed if info about the incident became public and, therefore, decided not to provide notification as required by 164.400 et seq.”

(75 FR 40879)

- Beware missing PHI or unencrypted devices (e.g., smartphones, laptops, USBs, etc.) containing PHI.

# 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.)

# Notice to Individual: Timing

- **Must provide notice without unreasonable delay and in no case later than 60 calendar days after discovering breach.**
  - Deemed to have discovered breach the first day your workforce member or agent (other than violator) knew or should have known of breach.
  - Must conclude investigation and send notice promptly; cannot wait until end of 60 days if circumstances do not warrant.

(45 CFR 164.404)

- **Train workforce to report promptly.**
- **Require business associates to report promptly.**

# Notice to Individual: Content

- Brief description of what happened, including dates of breach and discovery.
- Description of types of unsecured PHI that were involved (e.g., name, SSN, DOB, address, account number, etc.).
- Steps persons should take to protect themselves from harm resulting from breach.
- Brief description of what covered entity is doing to investigate, mitigate, and protect against future breaches.
- Contact procedures to ask questions or learn info, including toll-free phone number, e-mail address, website, or postal address.

(45 CFR 164.404(c)).

# Notice to Individual: Method

- **Written notice to individual**
  - By first-class mail to last known address.
  - By e-mail if individual has agreed.
- **If individual is deceased and covered entity has address for next of kin or personal rep,**
  - By first class mail to—
    - Next of kin, or
    - Personal representative under HIPAA
- **In urgent situations, may also contact by phone or other means, but must still send written notice.**

(45 CFR 164.404(d))

# Substitute Notice

- **If lack sufficient contact info to provide written notice to individual, must provide substitute form reasonably calculated to reach the individual.**
  - **If less than 10 such persons, then may use alternative form of written notice, telephone, or other means.**
  - **If 10 or more such persons, then must:**
    - **Conspicuous post on covered entity's website for 90 days or in major print or broadcast media where affected individuals likely reside, and**
    - **Include toll-free number for at least 90 days.**

(45 CFR 164.404(d))

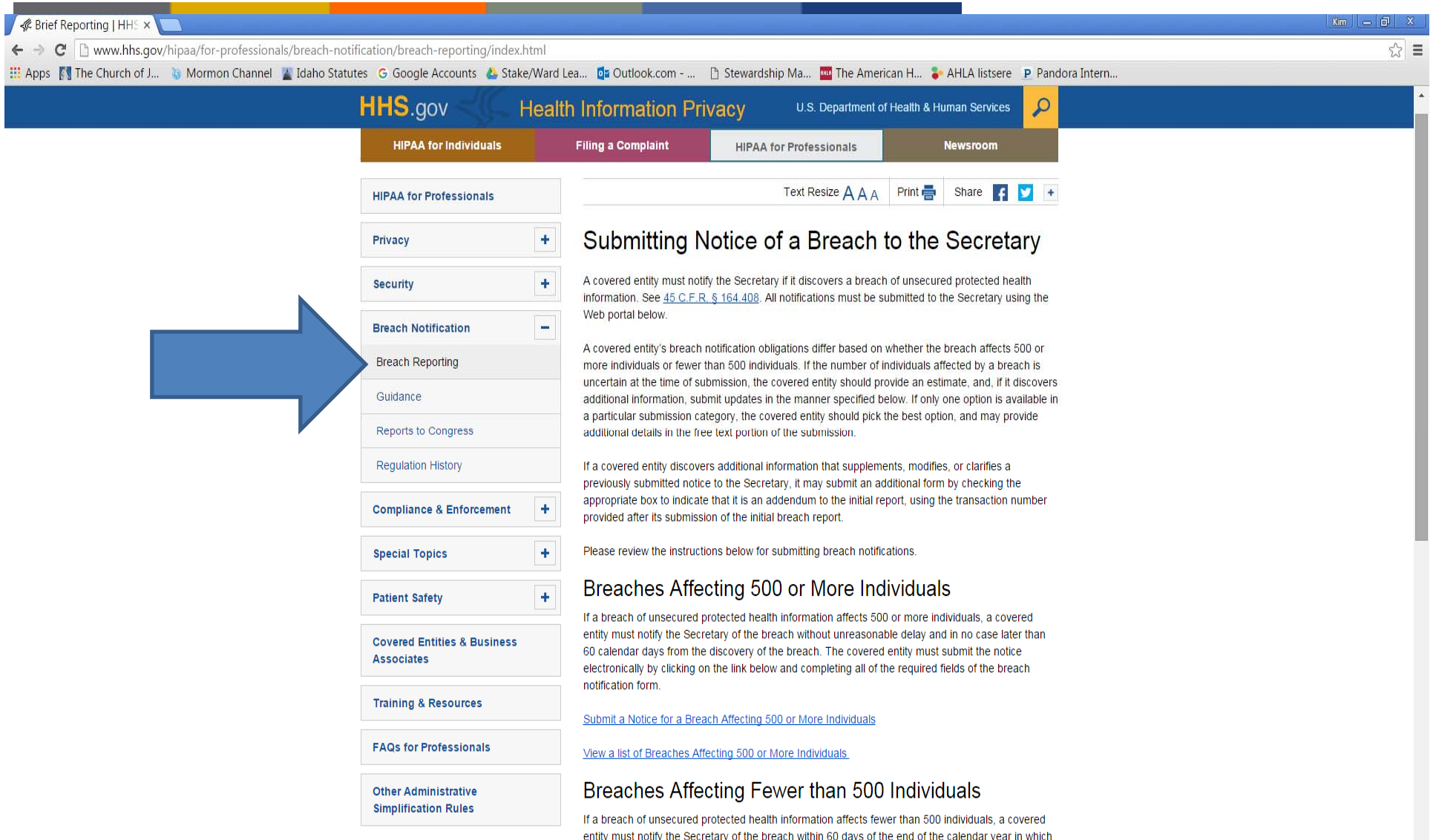
# Notice to HHS

- 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>



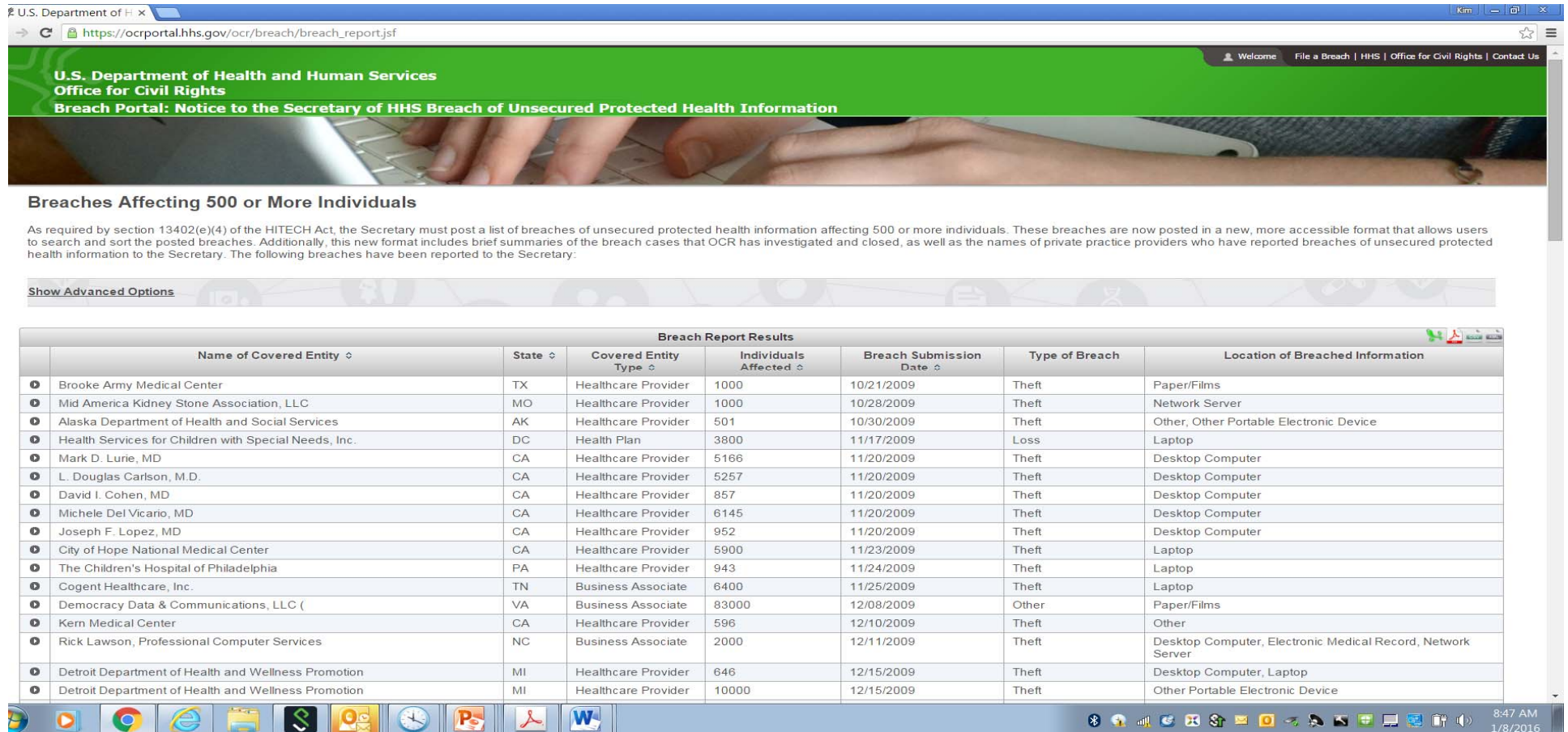
The screenshot shows the HHS.gov website with the following elements:

- Header:** HHS.gov Health Information Privacy U.S. Department of Health & Human Services
- Navigation:** HIPAA for Individuals, Filing a Complaint, HIPAA for Professionals, Newsroom
- Left Sidebar:** HIPAA for Professionals, Privacy (+), Security (+), Breach Notification (-), Breach Reporting (highlighted with a blue arrow), 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
- Main Content:**
  - Text:** Text Resize A A A, Print, Share (Facebook, Twitter, Plus)
  - Section Header:** Submitting Notice of a Breach to the Secretary
  - Text:** 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.
  - Text:** 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.
  - Text:** 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.
  - Text:** Please review the instructions below for submitting breach notifications.
  - Section Header:** Breaches Affecting 500 or More Individuals
  - Text:** 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.
  - Text:** [Submit a Notice for a Breach Affecting 500 or More Individuals](#)
  - Text:** [View a list of Breaches Affecting 500 or More Individuals.](#)
  - Section Header:** Breaches Affecting Fewer than 500 Individuals
  - Text:** 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)



The screenshot shows a web browser window displaying the HHS Breach Portal. The page title is "U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". Below the header, there is a section titled "Breaches Affecting 500 or More Individuals". A paragraph 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 "Show Advanced Options" link and a table titled "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.**

# <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

## **FACT SHEET: Ransomware and HIPAA**

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).<sup>1</sup> Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

### **1. What is ransomware?**

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates<sup>2</sup> data, or ransomware in conjunction with other malware that does so.

### **2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?**

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

# Ransomware: OCR Guidance

---

- Ransomware = reportable breach unless covered entity can demonstrate low probability that the data has been compromised considering:
  - Nature and extent of PHI affected;
  - Who used the PHI or to whom it was disclosed.
  - Whether PHI was actually acquired or viewed.
  - Extent that risk mitigated.

(See 45 CFR 164.402)

# Ransomware: OCR Guidance

---

- **Additional factors:**
  - Exact type and variant malware.
  - Algorithmic steps taken by malware.
  - Exfiltration attempts.
  - Risk of unavailability of data.
  - Threat to integrity of data, e.g., was original destroyed?
- **Conclusion:**
  - Implement required safeguards.
  - Regularly backup data.

# Idaho Identity Theft Statute (IC 28-51-104)



# 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)



# Action Items

## HIPAA Top 10 List



# HIPAA Action Items

---

1. Assign and document HIPAA responsibility.
  - Privacy officer
  - Security officer
2. Ensure the officers understand the rules.
3. Review security rule compliance.
  - Conduct and document security risk assessment.
  - Beware electronic devices.
4. Ensure you have required policies.
  - Privacy rule.
  - Security rule.
  - Breach notification rule.

# HIPAA Action Items

---

- 5. Develop and use compliant forms.**
  - Authorization, privacy notice, patient requests, etc.
- 6. Execute BAAs with business associates.**
  - Ensure they are independent contractors.
  - Follow up if there are problems with business associate.
- 7. Train members of workforce and document training.**
  - Upon hiring.
  - Periodically thereafter.
- 8. Use appropriate safeguards.**
  - Confidentiality agreements with workforce members.
  - Reasonable administrative, technical and physical safeguards.

# HIPAA Action Items

---

- 9. Respond immediately to any potential breach.**
  - Immediately take appropriate steps to mitigate.
  - Retrieve PHI.
  - Obtain assurances of no further use or disclosure.
  - Warn persons who received info of penalties of violations.
  - Investigate facts to determine if there was a reportable breach.
  - Sanction workforce member as appropriate.
  - Implement corrective action, additional training, etc.
  - Document foregoing.
- 10. Timely report breaches as required.**
  - To patient or personal representative.
  - To HHS.
  - Internal accounting of disclosure log.

# Additional Resources

---



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

The screenshot shows the HHS.gov website for HIPAA for Professionals. A blue arrow points from the URL above to the search bar. Another blue arrow points from the search bar to the 'HIPAA for Professionals' button in the main navigation. A third blue arrow points from the left side of the page to the 'HIPAA for Professionals' link in the left-hand menu.

**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](#)

Text Resize [A](#) [A](#) [A](#) Print  Share [f](#) [t](#) [+](#)

## 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](#).

**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

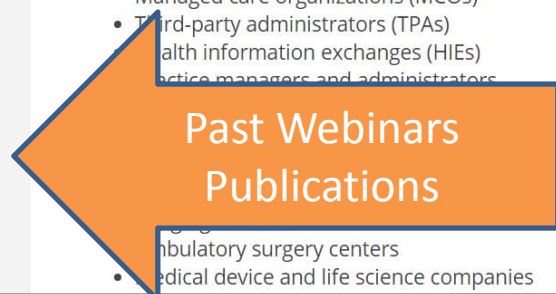
# HIPAA Resources

---

- **OCR website: [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)**
  - Regulations
  - Summary of regulations
  - Frequently asked questions
  - Guidance regarding key aspects of privacy and security rules
  - Sample business associate agreement
  - Portal for breach notification to HHS
  - Enforcement updates
- **OCR listserve**
  - Notice of HIPAA changes

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

The screenshot shows the top navigation bar with the text "EXCELLENCE IN LEGAL SERVICES" and the Holland & Hart logo, which includes a "70 YEARS EST. 1947" anniversary mark. A "MENU" button is visible on the left. The main content area is divided into several sections: "OVERVIEW" (with a right-pointing arrow), "PRACTICES/INDUSTRIES", "NEWS & INSIGHTS", "CONTACTS", and "HEALTH LAW BLOG". Under "CONTACTS", there are two profile cards for Kim Stanger (Partner, Boise) and Blaine Benard (Partner, Salt Lake City). The "HEALTH LAW BLOG" section includes a RSS icon and the text "Access to previous webinar recordings, publications, and more." The right side of the page features a main heading "The Healthcare Industry is po this sector now making up cl stand ready to help as chang" and a sub-heading "Clients We Serve" followed by a bulleted list of client types. At the bottom of the page, there is a "Most Popular Stories" section. The Windows taskbar at the bottom shows various application icons and the system clock indicating 7:34 AM on 2/8/2017.





# Questions?

---



**Kim C. Stanger**  
**Holland & Hart LLP**  
**(208) 383-3913**  
**[kcstanger@hollandhart.com](mailto:kcstanger@hollandhart.com)**