



Identifying and Responding to HIPAA Breaches

Kim C. Stanger
(2-16)

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.

Preliminaries

- Written materials
 - .ppt presentations
 - Article, *Responding to HIPAA Violations*
 - Sample Breach Notification Policy
- Presentation will be recorded and available for download at www.hhhealthlawblog.com.
- If you have questions, please submit them using chat line or e-mail me at kcstanger@hollandhart.com.

Preliminaries

- **We will focus on HIPAA violations.**
 - HIPAA preempts less restrictive laws.
- **Beware additional state laws.**
 - Medical privacy laws.
 - Data breach notification laws.
- **Beware additional contract terms.**
 - Business associate agreements.
 - Confidentiality agreements.

Health Insurance Portability and Accountability Act, 42 CFR part 164



HIPAA Overview

- **Privacy Rule, 45 CFR 164.500 et seq.**
 - Requires covered entities and business associates to protect the confidentiality of protected health information (“PHI”)
 - Gives patients certain rights concerning their PHI.
- **Security Rule, 45 CFR 164.300 et seq.**
 - Requires covered entities to implement certain safeguards to protect e-PHI.
- **Breach Notification Rule, 45 CFR 164.400 et seq.**
 - Requires covered entities and business associates to self-report breaches of unsecured PHI.
- **Omnibus Rule changed the rules.**

HIPAA Penalties

HIPAA

**Business
Associates**

**Covered
Entities**

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">• \$50,000 fine• 1 year in prison
Committed under false pretenses	<ul style="list-style-type: none">• 100,000 fine• 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	<ul style="list-style-type: none">• \$250,000 fine• 10 years in prison

Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none">• \$100 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Violation due to reasonable cause	<ul style="list-style-type: none">• \$1000 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none">• \$10,000 to \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none">• At least \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory

Civil Penalties

- **HHS may not impose a civil penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes that the violation is:**
 - **Not due to willful neglect, and**
 - **Corrected within either the 30-day period beginning on the first date the covered entity or business associate knew or should have known that the violation occurred, or such additional time as HHS deems appropriate based on the facts.**

(45 CFR 160.410(b))

Civil Penalties

- **“Willful neglect” = conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA rule that was violated.**

(45 CFR 160.401)

- **HHS gave the following examples of “willful neglect”:**
 - **“Fail[ure] to implement any policies and procedures to reasonably and appropriately safeguard PHI....”**
 - **“Fail[ure] ... to respond to incidents as required by [the Breach Notification Rule]....”**

(75 FR 40879)

Civil Penalties

- HHS indicated the following represents a situation where the covered entity did not act with willful neglect:

“A hospital employee accessed the paper medical record of his ex-spouse while he was on duty..., knowing that such access was not permitted by the Privacy Rule and contrary to the policies and procedures of the hospital.... The covered entity had appropriate and reasonable safeguards regarding employee access to medical records, and that it had delivered appropriate training to the employee.”

(75 FR 40879)

- No willful neglect = no penalties, if covered entity corrects the situation within 30 days.

Civil Penalties



- **Key to avoiding HIPAA penalties:**
 - Have required policies and safeguards in place.
 - Train your personnel and document training.
 - Respond promptly and appropriately to suspected violations.

HIPAA Settlements in 2015

Date	Fine	Party	Allegations
12/15	\$750,000	University of Washington Medical School	Failed to implement security rule policies and procedures
11/15	\$3,500,000	Triple-S Mgmt Co., an insurance holding	Failed to implement safeguards; improper disclosures; etc.
11/15	\$850,000	Lahey Hospital	Stolen laptop; inadequate security rule protections
8/15	\$750,000	Cancer Care Group	Stolen laptop; inadequate security rule protections
6/15	\$218,400	St. Elizabeth's Medical Ctr	Unsecure internet document sharing program; no security rule protection
4/15	\$125,000	Cornell Prescription Pharmacy	Improper disposal of paper records

Additional Reasons to Comply

- **State attorney general can bring lawsuit.**
 - \$25,000 fine per violation + fees and costs
- **Affected individuals may sue for violations.**
 - No private cause of action under HIPAA... yet.
 - But HIPAA may establish duty of care.
- **In the future, affected individuals may recover percentage of fines or penalties.**
 - Watch for new rule.
- **Must sanction employees who violate HIPAA.**
- **Covered entity must act to stop business associate's misconduct or terminate business associate agreement ("BAA").**
- **Covered entity may sue business associate for breaching the BAA.**
- **HHS is resuming audits.**

Additional Reasons to Comply

- **Must self-report certain HIPAA violations.**
 - To individual if he/she requests accounting of disclosures.
 - To covered entity if business associate violates HIPAA Privacy Rule BAA.
 - To patient, HHS, and perhaps local media if there is a “breach” of “unsecured PHI.”

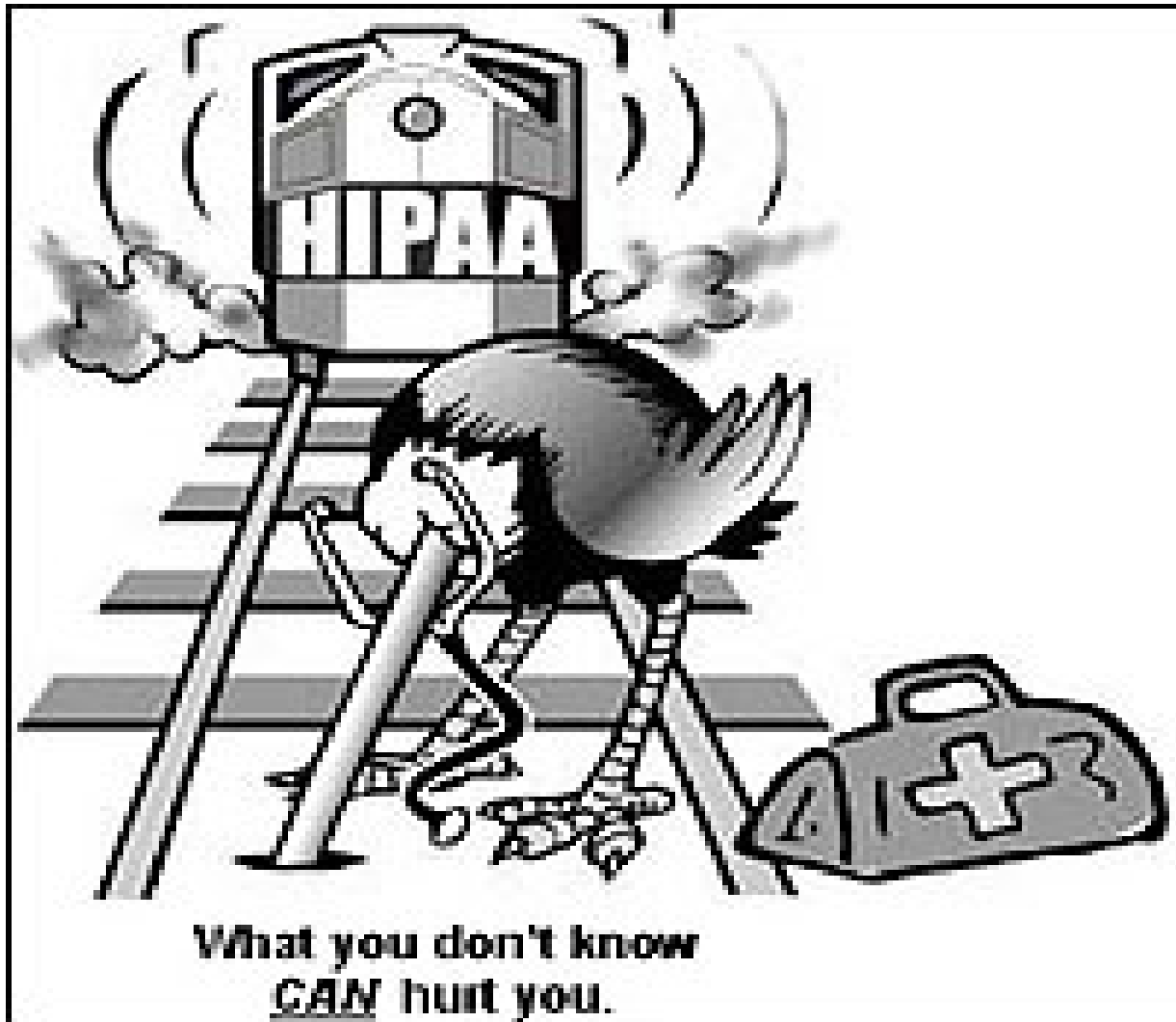
(45 CFR 164.404, .502(e), and .528)

- *More about this later...*

So you think you might have a HIPAA breach?



Do not do this...



1. Take immediate action to stop the breach.



- We'll come back to this...

2. Immediately report to privacy officer.

- **All covered entities must have a privacy officer and security officer designated in writing.**
- **Train staff to immediately report suspected breaches to the privacy officer.**
 - **Immediate response may help avoid breach reporting obligation and/or penalties.**
 - **May avoid penalties if correct violation within 30 days of when knew or should know of violation.**
 - **Must report breach within 60 days of when knew or should know of violation.**
 - **Business associate agreement may impose shorter deadlines.**
- **Privacy officer should investigate.**

3. Confirm whether HIPAA applies.

- Was the action taken by an entity acting in its capacity as either:
 - A covered entity.
 - Healthcare provider who engages in certain electronic transactions.
 - A health plan, including employee group health plan:
 - With 50 or more participants, or
 - Administered by a third party.
 - Business associate.
 - An entity that creates, maintains, transmits, or uses protected health info on behalf of a covered entity.

(45 CFR 160.103)

3. Confirm whether HIPAA applies.

- Is the info “protected health info”.
 - Created or received by a healthcare provider or health plan; and
 - Relates to the past, present or future health, healthcare or payment for healthcare; and either
 - Identifies the individual; or
 - There is reasonable basis to believe the info can be used to identify the individual.

- Not de-identified info.

(45 CFR 160.103, 164.514)

4. Confirm whether HIPAA violated.

- **Use, access or disclosure of PHI unless:**
 - For treatment, payment or healthcare operations so long as the covered entity did not agree to restrict such use or disclosure. (45 CFR 164.506 and .522)
 - For facility directory or to family member/person involved in healthcare or payment if patient did not object. (45 CFR 164.510)
 - Have written HIPAA-compliant authorization. (45 CFR 164.508)
 - Disclosure required by another law or satisfies another exception for certain public safety or government functions. (45 CFR 164.512)
- **Includes breaches by business associates and agents.**
(45 CFR 164.502)

4. Confirm whether HIPAA violated.

- Use, disclosure, or request for more PHI than the minimum necessary to accomplish the intent of a permitted use, disclosure or request.
- The “minimum necessary” standard does not apply to:
 - Disclosures to or requests by another healthcare provider.
 - Uses or disclosures made per an authorization.
 - Uses or disclosures required by law.

(45 CFR 164.502(b))

4. Confirm whether HIPAA violated.

- Incidental disclosures do not violate HIPAA and are not reportable.
- Incidental disclosure =
 - Incident to a use or disclosure that is otherwise permitted or required, and
 - The covered entity otherwise complied with
 - The “minimum necessary” standard, and
 - Implemented reasonable safeguards to protect against improper disclosures.

(45 CFR 164.502(a)(1))

4. Confirm whether HIPAA violated.

- “An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Rule”, e.g.,
 - A hospital visitor may overhear a provider’s confidential conversation with another provider or a patient, or
 - A hospital visitor may glimpse a patient’s PHI on a sign-in sheet or nursing station whiteboard.
- Must use reasonable safeguards, e.g.,
 - Speak quietly or do not discuss PHI in public areas.
 - Do not use patients’ names in public areas.
 - Isolate or lock file cabinets or records rooms.

(OCR Website, “Incidental Disclosures”)

5. Check on insurance.

- Many companies carry cyberliability or other potentially applicable insurance.
- Check with broker.
- When in doubt, report.
 - Delay in reporting may give insurer excuse to deny coverage.
 - Insurer may accept coverage despite terms in policy.
 - Insurer may provide resources to help you respond.
- Document communications with insurer.

6. Investigate promptly.

- **Confirm facts with person(s) involved.**
 - Person who committed alleged violation.
 - Person(s) who may have received PHI improperly.
 - Witnesses.
- **Confirm reason for use or disclosure.**
- **Confirm what info accessed, used or disclosed.**
- **Confirm scope of access, use or disclosure.**
- **Confirm no further access, use or disclosure made.**
- **Determine what steps should be taken to mitigate or correct the situation.**
- **Document investigation.**

7. Mitigate harm.

- A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure by the covered entity or its business associate of PHI in violation of its policies or the privacy rule.

(45 CFR 164.530(f))

- If a covered entity or business associate knows of a pattern or practice or a business associate or subcontractor that violates HIPAA, they must either:
 - Take steps to cure the breach or end the violation, or
 - Terminate the BAA.

(45 CFR 164.504(e))

7. Mitigate harm.

- Stop any further breaches.
- Retrieve, delete, and/or destroy PHI.
- Contact recipient(s) to confirm scope of uses or disclosures and warn against future uses and disclosures.
- Terminate access, change passwords, etc.
- Remote wipe any hard drives or mobile devices.
- Maybe notify affected individuals [discussed later].
- Maybe cover cost of additional measures such as credit reporting agency.
- Document actions.
 - HIPAA investigation file.
 - Letters to persons involved confirming facts and warnings.

8. Sanction employees.

- A covered entity must have policies and apply appropriate sanctions against members of its workforce who fail to comply with HIPAA rules or privacy policies.
- Document the sanctions.

(45 CFR 164.530(e)).

8. Sanction employees.

- **The sanctions should fit the crime, e.g.,**
 - Written warning
 - Suspension
 - Mandatory training
 - Termination
 - Report for government action
- **Sanctions may depend on:**
 - Intent.
 - Seriousness of breach.
 - Repeated misconduct.
 - Any other relevant factors.
- **Check employee policies.**

9. Correct the violation.

- ***THIS IS REALLY IMPORTANT!***
- It is an affirmative defense to HIPAA penalties if the covered entity or business associate:
 - Did not act with willful neglect, and
 - Corrected the violation within 30 days.

(45 CFR 160.410)

9. Correct the violation.

- **HHS appears to interpret “corrected” broadly:**
“For example, in the event a covered entity’s or business associate’s noncompliant inadequate safeguards policies result in an impermissible disclosure, the disclosure violation itself could not be fully undone or corrected. The safeguards violation, however, could be ‘corrected’ in the sense that the noncompliant policies and procedures could be brought into compliance.”

(75 FR 40879)

9. Correct the violation.

- Mitigate the harm, as discussed above.
- Sanction employees, as discussed above.
- Revise policies and procedures.
- Implement new or different safeguards.
- Train personnel.
- Enforce the policies and rules.
- Maybe notify affected individuals [discussed later]
- Take other appropriate steps.
- Document actions.

10. Log the improper disclosure.

- Patient has a right to request an accounting of certain disclosures of PHI by covered entity or business associate made during prior 6 years:
 - Disclosures in violation of HIPAA.
 - Disclosures for certain government functions under 45 CFR 164.512.

(45 CFR 164.528)

- “Disclosure” = release, transfer, provision of, access to, or divulging in any other manner of info outside the entity holding the info.

(45 CFR 160.103).

10. Log the improper disclosure.

- **Must include the following info in accounting:**
 - Date of the disclosure.
 - Name and address of the entity who received the PHI.
 - Brief description of the PHI disclosed.
 - Brief statement of the purpose of the disclosure or copy of written request for disclosure.

(45 CFR 164.528)

- **As a practical matter, this will require covered entities and business associates to maintain a log of disclosures.**

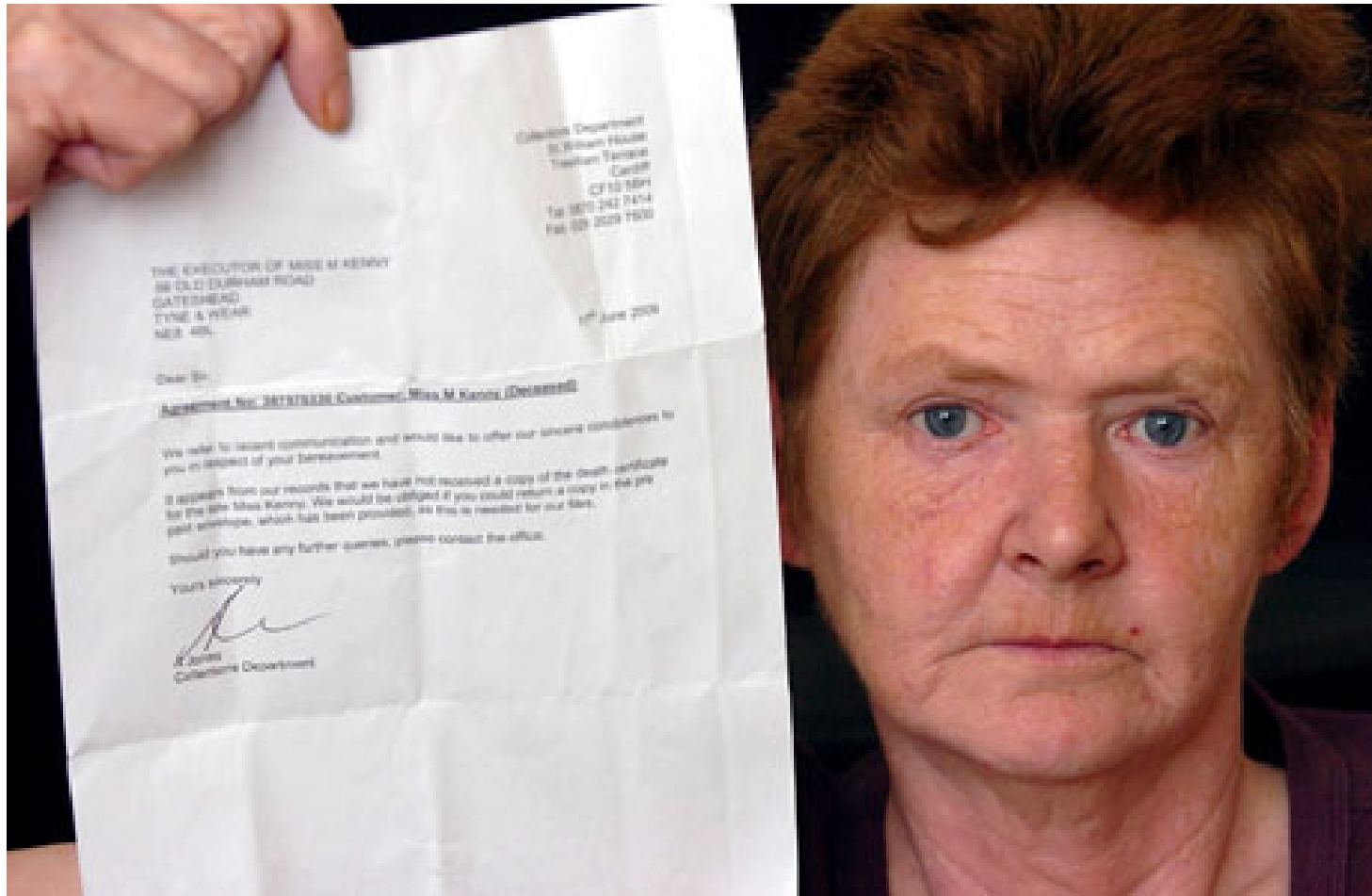
10. Log the improper disclosure.

- **Proposed Rule would expand the accounting of disclosure requirements if covered entity maintains electronic health records.**
 - **Must account for uses or disclosures for treatment, payment and healthcare operations.**
 - **Must provide report of access.**
- **The good news:**
 - **Only required to provide accounting of disclosure to patient if requested by individual.**
 - **Most individuals do not request accountings.**
- **Business associate agreement may have additional requirements.**

11. BA report to covered entity.

- **Business associate must report the following to the covered entity:**
 - Any use or disclosure of PHI not provided for by the BAA of which it becomes aware.
 - Any security incident of which it becomes aware, i.e., “attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an info system.”
 - Breaches of unsecured PHI per the Breach Notification Rule.
- (45 CFR 164.314(a), .410, and .504(a)(2))
- **Business associate agreements often contain additional requirements.**

12. Report per breach notification rule, if required.



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.
- **Guidance updated annually.**

(74 FR 42742 or 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)

When is PHI “Compromised”?

- Does “compromised” mean that the PHI is acquired, accessed, used or disclosed?
 - HHS recognized that requiring notice in all situations where PHI was accessed, acquired, used or disclosed would be too burdensome and would unduly trouble patients.
 - HHS noted “there are situations in which unauthorized acquisition, access, use or disclosure of [PHI] is so inconsequential that it does not warrant notification.”
 - Whether the PHI was actually acquired or viewed is only one factor in the risk assessment.

“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

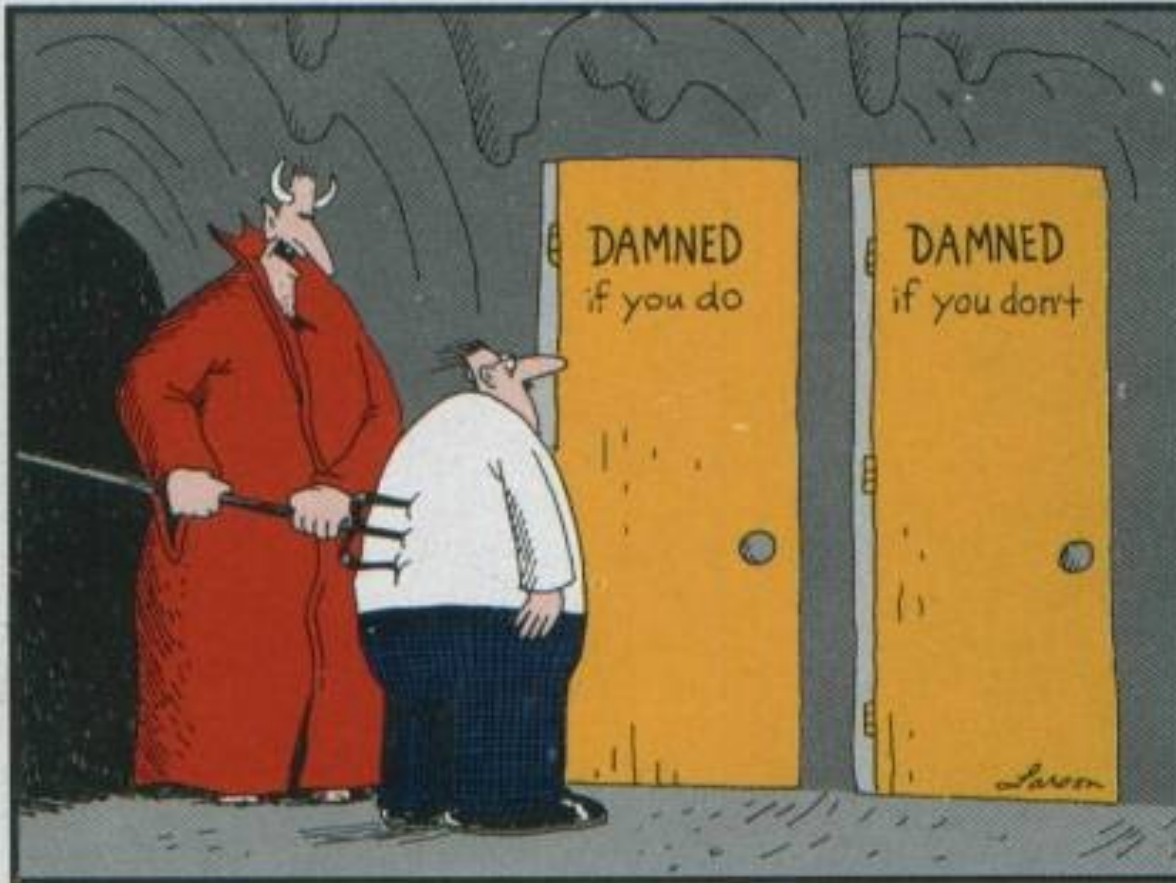
- **Until we receive further clarification, safer to err on the side of reporting all but clearly “inconsequential” breaches.**
 - Covered entity has burden of proving “low probability that PHI has been compromised.”
 - Failure to report may be viewed as willful neglect resulting in mandatory penalties.

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 devices containing PHI.

Breach of Unsecured PHI: Summary

- Reporting may reduce risk of significant penalties:
 - Willful neglect and mandatory penalties.
 - Excessive penalties.
- Reporting will increase risk of:
 - OCR investigation, which may uncover other problems.
 - Patient complaints or suits.
 - AG suits.
 - Costs of reporting.



"C'mon, c'mon — it's either one or the other."

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>.

[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



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](#)

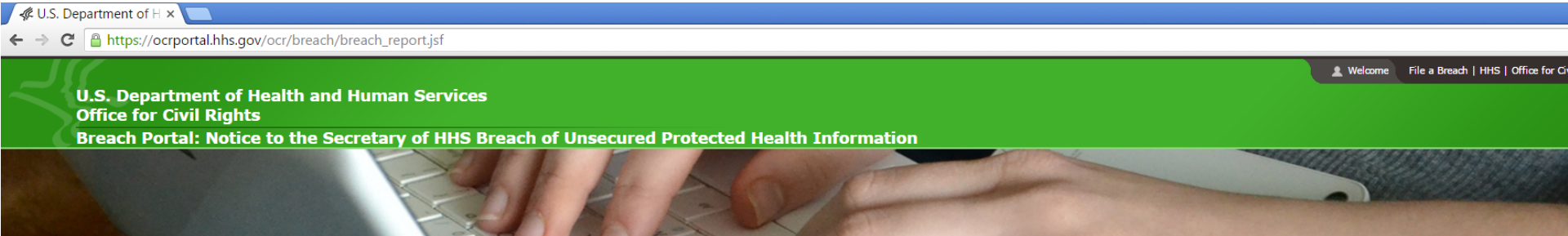
[View a list of Breaches Affecting 500 or More Individuals](#)

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 the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than

Notice to HHS

- HHS posts list of those with breaches involving more than 500 at 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 you 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

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.**

Delay by Law Enforcement

- **Law enforcement may delay notice if notice would impede criminal investigation or damage national security.**
 - **If stated in writing, covered entity or business associate shall delay notice accordingly.**
 - **If stated orally, covered entity or business associate shall—**
 - **Document statement and identity of law enforcement official making statement.**
 - **Delay notice for no more than 30 days unless written statement is given.**

(45 CFR 164.412)

To summarize...



<http://adiart.us>

If you think you have a breach

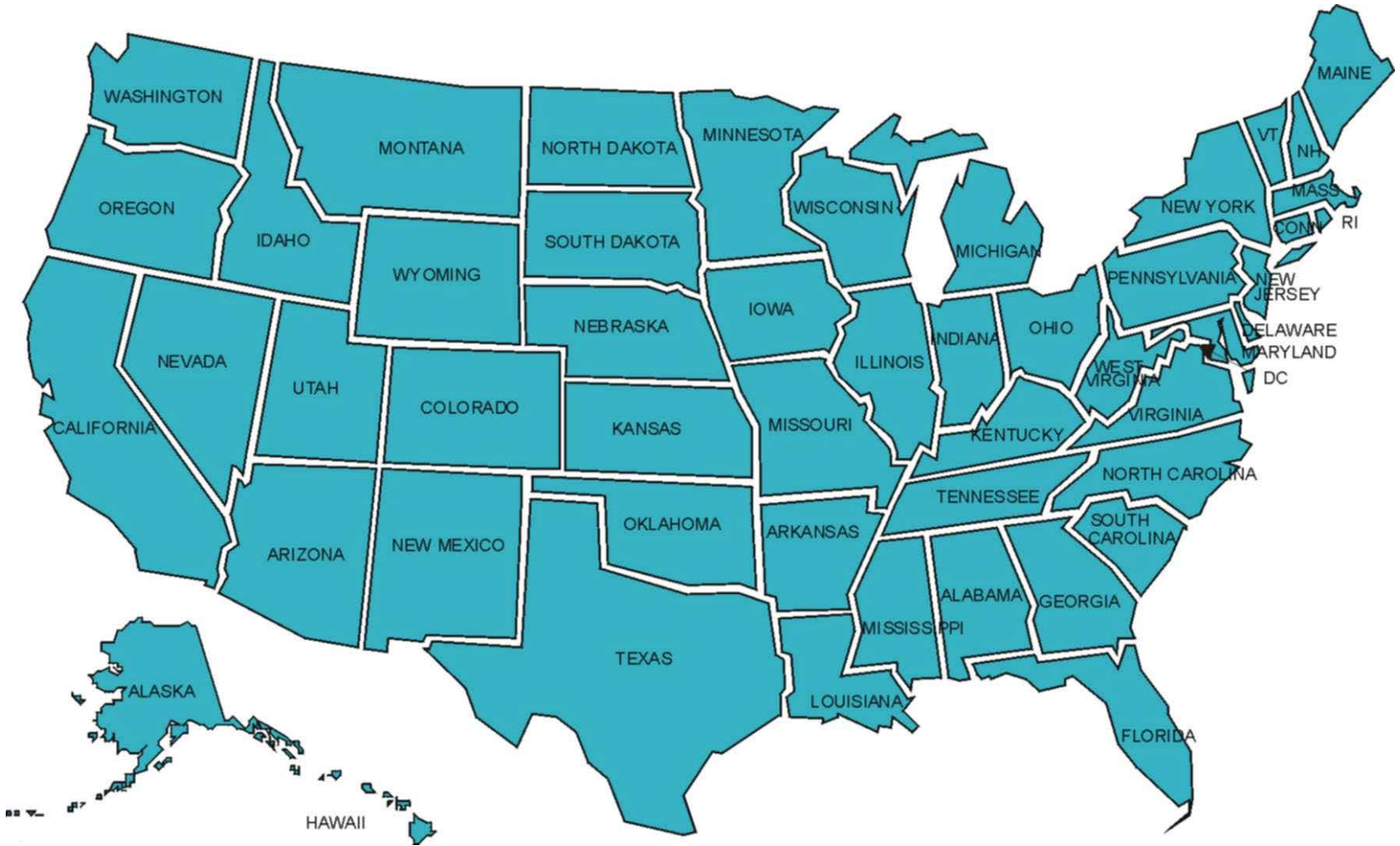
1. Act immediate action to minimize breach.
 2. Notify privacy officer.
 3. Confirm whether HIPAA applies.
 4. Confirm whether HIPAA was violated.
 5. Check on insurance.
 6. Investigate promptly.
 7. Mitigate any harm.
 8. Sanction workforce members.
 9. Correct any process that resulted in improper disclosures.
 10. Log the improper disclosure.
 11. Report if required.
 12. Document the foregoing.
- **Remember: prompt action may allow you to—**
 - Satisfy your duty to mitigate.
 - Avoid disclosure and breach reporting obligation.
 - Defend against HIPAA penalties.

To determine if breach is reportable

1. Was there unauthorized access, use or disclosure of unsecured PHI?
2. Did it violate the privacy rule?
3. Does one of the exceptions apply, e.g.,
 - Unintentional access by workforce member within job duties + no further violation.
 - Inadvertent disclosure to another person authorized to access PHI + no further violation.
 - Improbable that PHI may be retained.
4. Is there a low probability that the data has been compromised?
 - Risk assessment

** Document foregoing.*

Check additional state laws...



Responding to Possible HIPAA Violations



A GOOD OFFENSE IS YOUR BEST DEFENSE

Minimizing Exposure

- Act to minimize exposure before a violation occurs.
 - Know the rules.
 - Implement required policies and safeguards.
 - Train employees re policies and safeguards.
 - Execute confidentiality agreements and BAAs.
 - Respond immediately to a suspected breach.
 - Document foregoing.

Minimizing Exposure

- **If OCR initiates investigation:**
 - Consider contacting knowledgeable healthcare attorney.
 - Cooperate, but be careful what you disclose.
 - Explain your position in your response, including:
 - We had appropriate policies.
 - We had appropriate training.
 - Employee violated our policies and training.
 - We responded immediately and appropriately to mitigate any harm.
 - We have taken corrective actions.
 - Cite commentary and rules confirming no penalties in these situations.

Additional Resources

A person wearing a black long-sleeved shirt is holding a large red sign with white text. The sign reads "HELP WANTED" in bold, white, sans-serif capital letters. The person's hands are visible on the left and right sides of the sign, holding it steady. The background is plain white.

**HELP
WANTED**

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

Print

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

HIPAA Resources

- **OCR website: 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

Holland & Hart Resources

- www.hollandhart.com/healthcare
 - Webinar recordings
 - Articles
 - Forms
 - Checklists





people

practices

firm

locations

news & resources

blogs

careers

diversity & inclusion

community

Contact

Disclaimer

Site Map

Healthcare

Overview

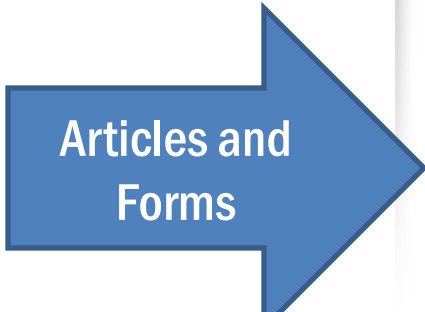
Holland & Hart provides a comprehensive health law practice serving the dynamic healthcare industry. In recent years, health care has changed, extraordinary competition, and increasingly complex regulatory requirements. Our attorneys and staff skillfully respond to these challenges. As a result of our expertise in healthcare law, we are able to provide coordinated services to meet the business, transactional, litigation, and regulatory needs of our clients.

Our healthcare clients include hospitals, individual medical providers, medical groups, managed care organizations (MCOs), third-party administrators (TPAs), health information exchanges (HIEs), practice managers and administrators, independent practice associations (IPAs), owners of healthcare assets, imaging centers, ambulatory surgery centers, medical device and life science companies, rehabilitation centers, and extended and eldercare facilities. We have also assisted clients with the significant changes enacted by the Affordable Care Act, including advice regarding employer and health plan compliance, health insurance exchanges, accountable care organizations, and nonprofit cooperative health plans.

[+ Read More](#)



View our [blog](#) and [webinar recordings](#) that cover HIPAA, antitrust, compliance, and more!



Articles and
Forms

- Publications

HIPAA Privacy Rule Modified to Permit Covered Entities to Make Certain Limited Disclosures to the National Instant Criminal Background System

[+ Expand All](#)

Future Webinars



- *Health Law Basics* monthly webinar series
 - 2/25/16 New Repayment Rule

- *Healthcare Update* and *Health Law Blog*
 - Under “Publications” at www.hollandhart.com.
 - E-mail me at kcstanger@hollandhart.com.

Questions?

Kim C. Stanger
Holland & Hart LLP
(208) 383-3913

kcstanger@hollandhart.com



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.