



Identifying and Responding to HIPAA Breaches

Kim C. Stanger

(2-17)

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.

Holland & Hart Webinar Series

Our 2017 HIPAA Compliance Webinars:

- 12/22/16 Risk Assessments
- 2/7/17 Security Rule
- 2/9/17 Privacy Rule
- 2/16/17 Business Associates
- 2/23/17 Responding to Breaches**



Webinars and materials are available at

[http://www.hhhealthlawblog.com/webinar-recordings-and-presentations.](http://www.hhhealthlawblog.com/webinar-recordings-and-presentations)

Overview

- Practical suggestions for responding to HIPAA breaches
- Reporting breaches
 - Covered entity reporting obligations
 - BAA reporting obligations
- OCR's Ransomware Guidance
- State breach notification laws



Preliminaries

- Written materials
 - .ppt presentations
 - 45 CFR 164.400 *et seq.*
 - Stanger, *Responding to HIPAA Violations*
 - Stanger, *Sample Breach Notification Policy*
 - OCR, *Fact Sheet: Ransomware and HIPAA*
- 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 (“HIPAA”)

- 45 CFR 164
 - .300: Security Rule
 - .400: Breach Notification Rule
 - .500: Privacy Rule



HIPAA Penalties



HIPAA

**Covered
Entities**

**Business
Associates**

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

“Willful Neglect”

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

(45 CFR 160.401)

- **E.g., “A covered entity’s employee lost an unencrypted laptop that contained unsecured protected health information. HHS’s investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq.”**


(75 FR 40879)

HIPAA Fines/Settlements Over Last Year

Conduct	Penalty
Unauthorized access to records of 115,000 patients through former employee's login	\$5,500,000
Loss or theft of unencrypted devices containing info of 7,000 patients; failure to take timely action in response	\$3,200,000
Theft of unencrypted USB containing info of 2,200 individuals	\$2,200,000
Failure to timely report breaches	\$475,000
Malware exposed info of 1,600 persons	\$650,000
Patient info accessible through internet searches	\$2,140,500
Loss of unencrypted backup tapes by BA; CE failed to update BAA	\$400,000
Numerous breaches involving 4,000,000 persons	\$5,500,000
Theft of unencrypted laptop exposing info of 10,000 patients	\$2,750,000
BA lost x-rays of 17,300 patients; CE failed to have BAA	\$750,000
Stolen unencrypted laptop containing info of 13,000 patients	\$3,900,000
BA's laptop containing 9,400 patients' info stolen; no BAA	\$1,550,000

y action risks security and costs money

Text Resize **A A A**

Print 

Share   


FOR IMMEDIATE RELEASE
February 1, 2017

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

Lack of timely action risks security and costs money

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) civil money penalty against Children’s Medical Center of Dallas (Children’s) based on its impermissible disclosure of unsecured electronic protected health information (ePHI) and non-compliance over many years with multiple standards of the HIPAA Security Rule. OCR issued a Notice of Proposed Determination in accordance with 45 CFR 160.420, which included instruction for how Children’s could file a request for a hearing. Children’s did not request a hearing. Accordingly, OCR issued a Notice of Final Determination and Children’s paid the full civil money penalty of \$3.2 million. Children’s is a pediatric hospital in Dallas, Texas, and is part of Children’s Health, the seventh largest pediatric health care provider in the nation.

 [top](#)

Text Resize **A A A**Print Share   **FOR IMMEDIATE RELEASE**

January 9, 2017

Contact: HHS Press Office

202-690-6343

media@hhs.gov

First HIPAA enforcement action for lack of timely breach notification settles for \$475,000

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced the first Health Insurance Portability and Accountability Act (HIPAA) settlement based on the untimely reporting of a breach of unsecured protected health information (PHI). Presence Health has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying \$475,000 and implementing a corrective action plan. Presence Health is one of the largest health care networks serving Illinois and consists of approximately 150 locations, including 11 hospitals and 27 long-term care and senior living facilities. Presence also has multiple physicians' offices and health care centers in its system and offers home care, hospice care, and behavioral health services. With this settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether.

On January 31, 2014, OCR received a breach notification report from Presence indicating that on October 22, 2013, Presence discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from the Presence Surgery Center at the Presence St. Joseph

Avoiding HIPAA Penalties



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

So you think you might have a HIPAA breach?



Do not do this...



1. Take immediate action to stop the breach.


**KEEP
CALM
AND
MITIGATE
THE RISKS**



- 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.
 - A business associate of covered entity.
 - 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.

- **Did it involve protected health info (“PHI”).**
 - 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 covered entity did not agree to restrict such use or disclosure. (45 CFR 164.506, .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 or written patient request to disclose PHI. (45 CFR 164.508, .524)
 - 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.

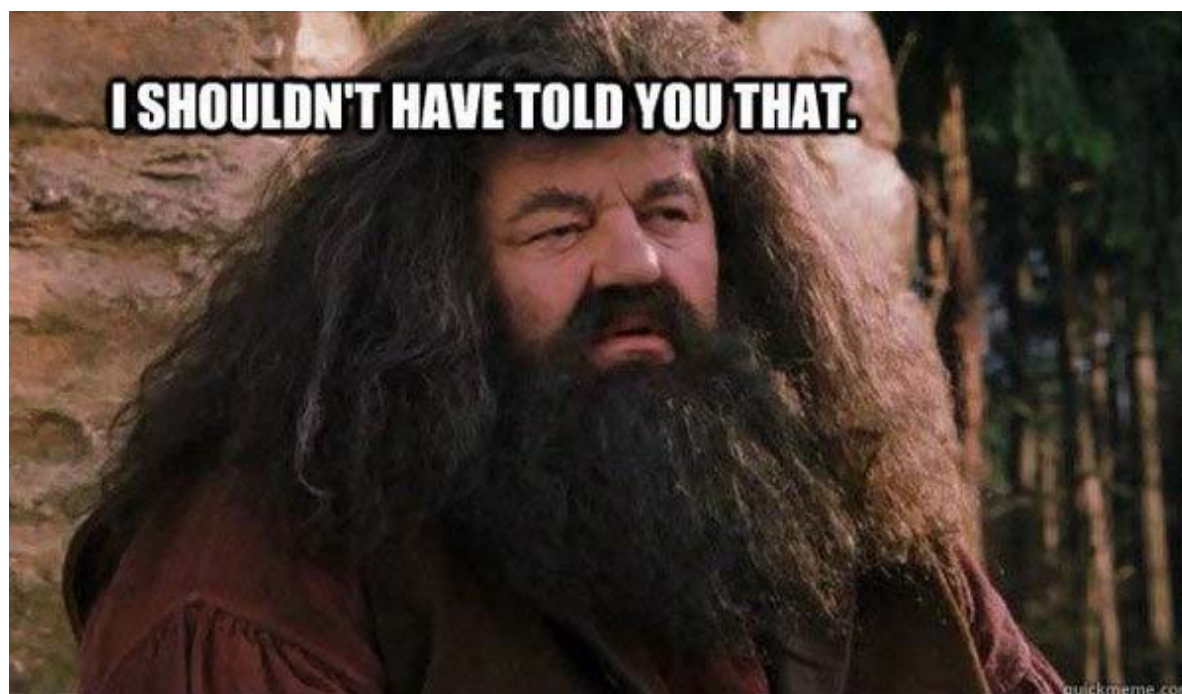
(OCR Website, “Incidental Disclosures”)

5. 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.**

5. Investigate promptly.

- *Don't make matters worse by disclosing PHI during your investigation!*



- Gather info, don't disclose it.

6. 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); see also 164.308(a)(6))

- **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))

6. 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.

7. 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)).

7. 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.

8. 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)

8. 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)

8. 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.

9. 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.

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.

(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 unencrypted devices (e.g., smartphones, laptops, USBs, etc.) 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.

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

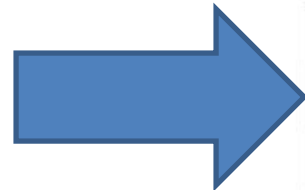


Covered Entities & Business Associates

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](#)

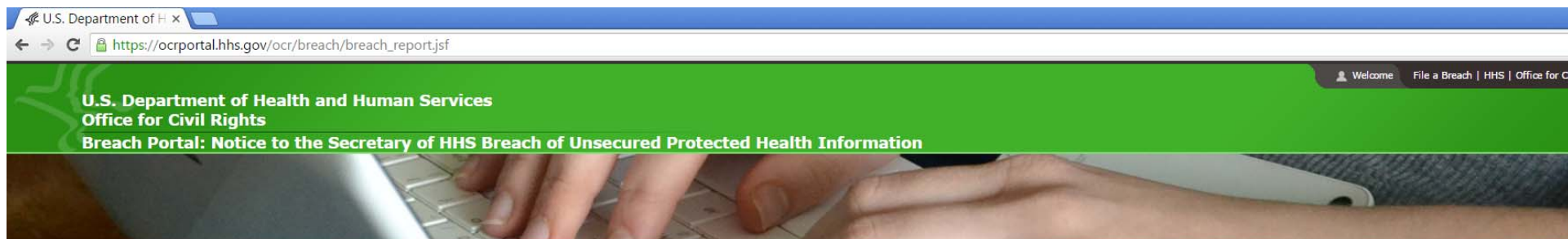
[View a list of Breaches Affecting 500 or More Individuals](#)

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

Ransomware



Health Information Technology

Hospitals are hit with 88% of all ransomware attacks

Written by Max Green | July 27, 2016 | [Print](#) | [Email](#)

189

[in Share](#)

[Tweet](#)

36

Hospitals and health systems have more to lose than organizations in other sectors when it comes to hacks. Patient data sells for more money than any other kind of information on the black market. Adding insult to injury, a new report suggests that the healthcare industry is hit significantly harder by ransomware than in any other — 88 percent of attacks hit hospitals.

NBC NEWS HOME TOP VIDEOS DECISION 2016 MORE

TECH > SECURITY

GADGETS INTERNET INNOVATION MOBILE

TECH MAR 23 2016, 5:16 PM ET

Three U.S. Hospitals Hit in String of Ransomware Attacks

by CONNOR MANNION

SHARE [f](#) [t](#) [g+](#) [c](#)

Three U.S. hospitals were hit hard this week by "ransomware" attacks that brought down their systems — the latest providers of medical care to be targeted in this way.



Privacy & Security

Ransomware: See the 14 hospitals attacked so far in 2016

SHARE  Share 34



By [Jessica Davis](#) | October 05, 2016 | 12:13 PM



**Data Security—
What You Don't Know
Can Hurt You**

Find out at HIMSS17
Booth #1460



Privacy & Security

Healthcare top target for cyberattacks in 2017, Experian predicts

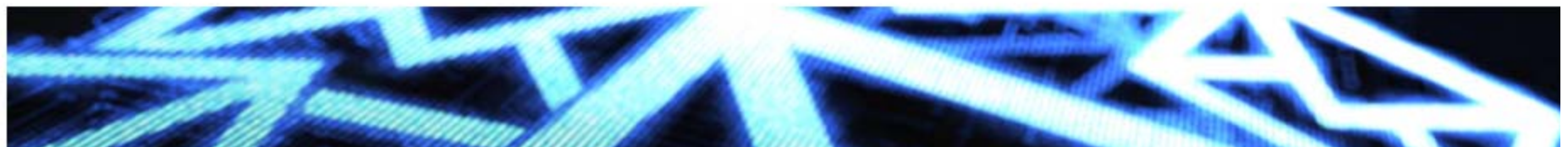
Ransomware is expected to become an even more insidious threat

By [Bernie Monegain](#) | December 01, 2016 | 11:08 AM

SHARE



118



<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).¹ 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: OCR Guidance

- **Suggestions for:**
 - Protecting against ransomware attacks through HIPAA compliance.
 - Identifying attacks.
 - Responding to attacks.

Ransomware: OCR Guidance

- **“When electronic (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a ‘disclosure’ not permitted under the HIPAA Privacy Rule.”**

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.

<https://www.justice.gov/criminal-ccips/file/872771/download>

m Ransomare - Adobe Acrobat Pro

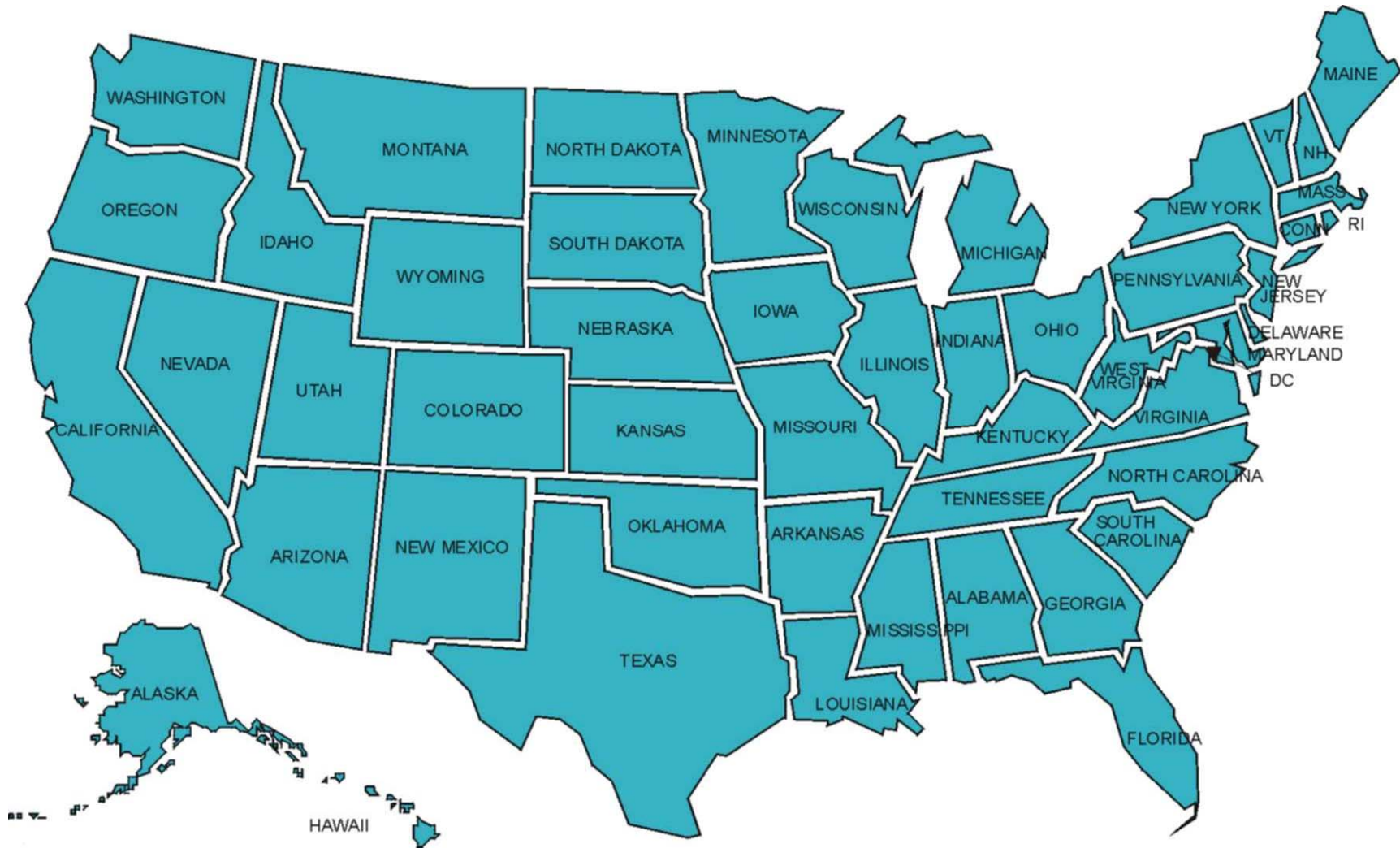
WorkSite



How to Protect Your Networks from

RANSOMWARE

Check additional state laws...





NCSL

NATIONAL CONFERENCE *of* STATE LEGISLATURES

[ABOUT US](#)

[LEGISLATORS & STAFF](#)

[RESEARCH](#)

[MEETINGS & TRAINING](#)

[NO](#)

SECURITY BREACH NOTIFICATION LAWS

1/4/2016

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of “personal information” (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of

[TABLE C](#)

[Security](#)

[Additiona](#)

[CONTA](#)

[Pam Gre](#)

State Data Breach Laws

- Often based on a model act that circulated a few years ago.
- Generally require 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, drivers license, credit card number + PIN or password, etc.)
 - Actual or reasonably likely misuse of personal info.
- \$25,000 fine if fail to notify persons.

(See, e.g., IC 28-51-104)

To summarize...



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.

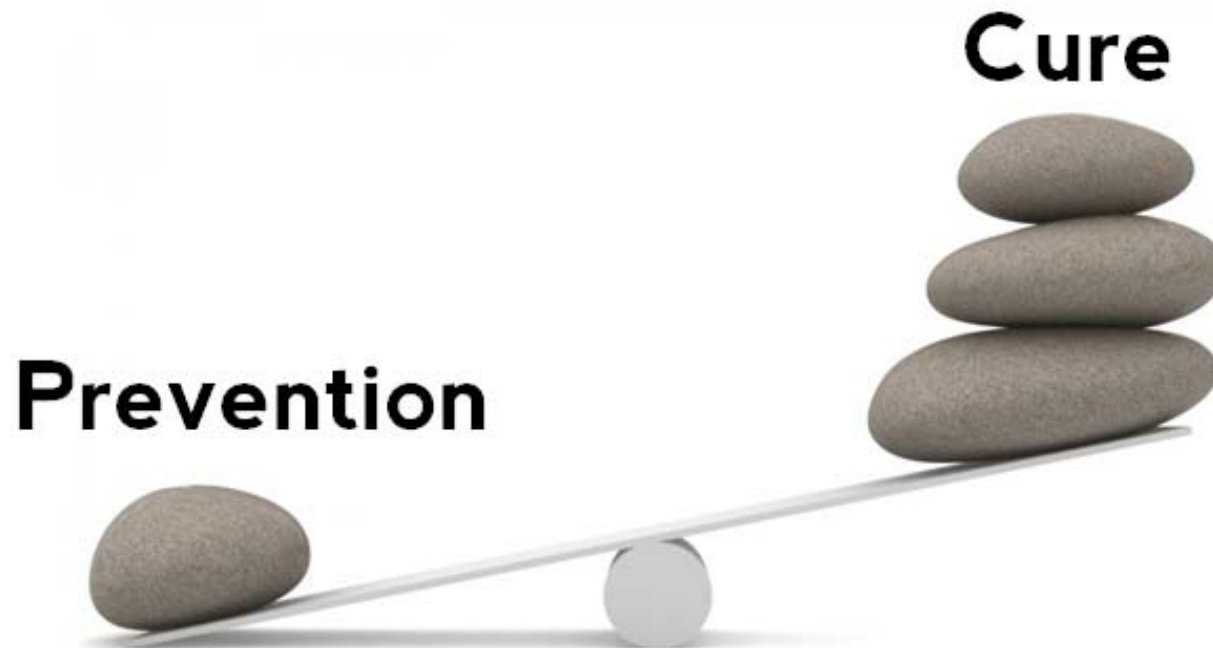
To determine if breach is reportable

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.*

Responding to Possible HIPAA Violations

- “An ounce of prevention is worth a pound of cure.”
– Benjamin Franklin



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



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

or Profession x

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

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...



HHS A-Z Index



HIPAA for Individuals



Filing a Complaint



HIPAA for Professionals



Newsroom

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

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business Associates

Training & Resources

FAQs for Professionals

Other Administrative Simplification Rules

Text Resize A A A

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

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

Healthcare | Holland & H x

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

EXCELLENCE IN LEGAL SERVICES



HOLLAND & HART



70 YEARS
EST. 1947

OVERVIEW ▶

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS



Kim Stanger
Partner
Boise



Blaine Benard
Partner
Salt Lake City



HEALTH LAW BLOG

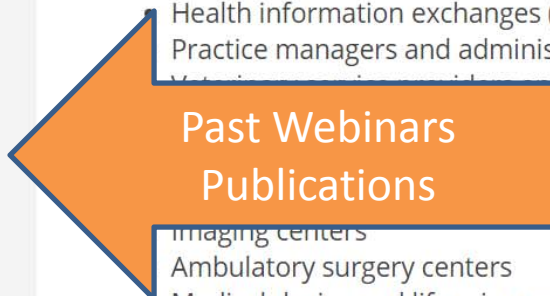
Access to previous webinar recordings, publications, and more.

The Healthcare
this sector now
stand ready to l

Issues such as rising
innovations in health
minds of many of ou
opportunities that a

Clients We Serve

- Hospitals
- Individual mec
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- Health information exchanges (HIEs)
- Practice managers and administrators
- Medical device and life science companies
- Imaging centers
- Ambulatory surgery centers
- Medical device and life science companies



Past Webinars
Publications

W
S

anc
in t
is a

Upcoming Holland & Hart Webinars

3/9 Cybersecurity in Healthcare

- To receive notices or client alerts, contact me at kcstanger@hollandhart.com



Questions?



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