




**HIPAA Privacy and Security Rules:
Overview and Update**



Kim C. Stanger
IHCA
Convention
(7/16)


HOLLAND & HART 

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 


**Health Insurance Portability and
Accountability Act (“HIPAA”)**

- 2003: Privacy Rules, 45 CFR 164.500
 - Requires covered entities to protect privacy of protected health info (“PHI”)
 - Gives patients certain rights concerning their info.
- 2005: Security Rules, 45 CFR 164.300
 - Requires covered entities to implement safeguards to protect electronic PHI.
- 2009: HITECH Act
 - Expanded and strengthened HIPAA.
- 2009: Breach Notification Rule, 45 CFR 164.400
 - Requires covered entities to report breaches of unsecured info.
- 2013: HIPAA Omnibus Rule, 78 FR 5566 (1/25/13)
 - Implemented and finalized HITECH Act requirements.

HOLLAND & HART 

Other Privacy Laws

- Must comply with other law if it is more strict than HIPAA, i.e.,
 - Provides greater protection to patient info.
 - Provides patients greater rights regarding their info.
- Other privacy laws:
 - Resident Rights, 42 CFR part 483
 - Idaho Licensing Regulations
 - Federally funded drug and alcohol treatment programs, 42 CFR part 2
 - Common law privacy rights.
 - Other?

HOLLAND & HART 

HIPAA Enforcement




HOLLAND & HART 

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

(42 USC 1320d-6(a)) 6 HOLLAND & HART 

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

(45 CFR 160.404) HOLLAND & HART

HIPAA Settlements this Year

Conduct	Settlement
Hospital allowed crew to film patients and gave unfettered access	\$2,200,000
Orthopedic group gave x-rays of 17,300 patients to vendor without business associate agreement	\$750,000
Hospital laptop containing 13,000 patients' info stolen from car	\$3,900,000
Business associate's laptop containing 9,400 patients' info stolen from business associate's car; no business associate agreement	\$1,550,000
PT clinic posted patient names, photos and testimonials on website	\$25,000
Employee left patient records behind when moved; investigation showed inadequate policies	\$239,800
Hospital employee downloaded malware exposing patient records	\$750,000
Health insurer failed to have risk analysis, policies, safeguards, etc.	\$3,500,000
Hospital laptop stolen from treatment room	\$850,000
Oncology group laptop and unencrypted backup media lost	\$750,000

Small hospice in Idaho pays \$50,000

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

FOR IMMEDIATE RELEASE
January 2, 2013

Contact: HHS Press Office
202-490-6343
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.


"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."

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.
 - Still waiting for regulations.
- 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.



Home > HIPAA/HITECH > HIPAA Violation Results in \$1.44 Million Jury Verdict Against Walgreens, Pharmacist

HIPAA Violation Results in \$1.44 Million Jury Verdict Against Walgreens, Pharmacist

By Cory J. Fox on August 14, 2013
Posted in HIPAA/HITECH, Medical Privacy


Although HIPAA does not create a private cause of action, a recent Indiana Superior Court jury verdict indicates that HIPAA could still play an important role in private causes of action in state court based on negligence and professional malpractice. In July 2013, a jury in Marion County, Indiana awarded \$1.44 million to a customer whose pharmacist accessed, reviewed, and used the information to intimate her. The customer filed suit against Walgreens, claiming that both parties had breached their duty of confidentiality and privacy. The complaint also included claims against the pharmacist and Walgreens for continuing to employ the pharmacist even after discovering the incident. The Court granted Walgreens' Motion for Summary Judgment on the negligent training claim.



On July 26, a jury in Marion County, Indiana awarded \$1.44 million to a customer whose pharmacist accessed, reviewed, and used the information to intimate her. The customer filed suit against Walgreens, claiming that both parties had breached their duty of confidentiality and privacy. The complaint also included claims against the pharmacist and Walgreens for continuing to employ the pharmacist even after discovering the incident. The Court granted Walgreens' Motion for Summary Judgment on the negligent training claim.

Other Cyberliability Laws

- Federal Trade Comm'n Act ("FTCA") § 5 (15 USC 45(a))
 - Prohibits unfair or deceptive acts affecting commerce.
 - Deceit = misrepresentations re privacy policy
 - Unfair = inadequate security measures
 - FTC has authority to regulate a company's cybersecurity efforts. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)
 - FTC has filed 50+ complaints against entities based on failure to safeguard personal info.

13 HOLLAND & HART 



The screenshot shows the Federal Trade Commission website page for the case "LabMD, Inc., In the Matter of". The page includes a search bar, navigation tabs (ABOUT THE FTC, NEWS & EVENTS, ENFORCEMENT, POLICY, TIPS & ADVICE, I WOULD LIKE TO...), and a "CASE SUMMARY" section. The summary states: "The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data."

Who and What Does it Cover?



HOLLAND & HART 

Entities Subject to HIPAA

- Covered entities
 - Health care providers who engage in certain electronic transactions.
 - 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.

HOLLAND & HART LLP

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 de-identified info.

HOLLAND & HART LLP


Prohibited Actions


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



HOLLAND & HART LLP


**Use and Disclosure Rules
(45 CFR 164.502-.514)**



HOLLAND & HART 

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 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 signed by patient that complies with 45 CFR 164.508.

HOLLAND & HART 

Treatment, Payment or Operations


- May use or disclose PHI without patient's authorization for:
 - Treatment
 - Payment
 - Health care operationsExcept psychotherapy notes.
- 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.
 - Don't agree! It increases liability.

(45 CFR 164.506 and 164.522)

HOLLAND & HART 


Persons Involved in Care

- May use or disclose PHI to family or others involved in patient's care or payment for care if conditions met.
 - 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)

HOLLAND & HART 


Safety and Govt Functions

- Authorization is not required if certain regulatory conditions are satisfied.
 - Avoid serious and imminent threat
 - Another law requires disclosure
 - Per court order, warrant or subpoena
 - Law enforcement if conditions satisfied
 - Public health activities
 - Health oversight activities
 - Workers compensation
 - Coroners
 - Persons in custody
 - Military purposes
- Check with privacy officer or 42 CFR 164.512 to determine if conditions are satisfied.
(45 CFR 164.512)

HOLLAND & HART 

Authorization

- May use or disclose PHI if have valid written authorization signed by patient or their personal representative.
- Authorization must contain elements and statements required in 45 CFR 164.508.
- Cannot combine HIPAA authorization with other consents or documents.
- Certain uses or disclosures require authorization.
 - Psychotherapy notes, except provider's use of own notes for treatment purposes.
 - For marketing purposes.
 - For sale of protected info.

HOLLAND & HART 

Disclosure Directed by Patient

- Individual or personal representative has right to direct that a copy of the record be transmitted to a third party.
- Written request signed by individual or personal representative and clearly identifies recipient and recipient's address.
 - Limits on charges apply.
 - Must transmit in manner, form and format requested if readily producible.
- Compare authorization:
 - Individual requests transmittal: individual request rules in 45 CFR 164.524 apply.
 - Third party requests transmittal: authorization rules in 45 CFR 164.508 apply.

(45 CFR 164.524; OCR Guidance on Access)

Verification

- Before disclosing PHI:
 - Verify the identity and authority of person requesting info if he/she is not known.
 - E.g., check the badge or papers of officers; birthdates or SSN for family; 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 164.512(f))

Minimum Necessary Standard


- Cannot use or disclose more than is reasonably necessary for intended purpose.
- Does not apply to disclosures to:
 - Patient
 - Provider for treatment
 - Per individual's authorization
- Must have policies regarding
 - Role-based access
 - Routine disclosures and requests for info

(45 CFR 164.502 and .514)

Personal Representatives

- Under HIPAA, you must treat the personal rep as if they were the patient.
- Personal reps generally have right to exercise patient rights, e.g.,
 - Request restrictions on use or disclosure of protected info.
 - Access protected info.
 - Amend protected info.
 - Obtain accounting of disclosures of protected info.
- Personal rep = persons with authority under state law to:
 - Make healthcare decisions for patient.
 - Make decisions for deceased patient's estate.


(45 CFR 164.502(g))

HOLLAND & HART 

Personal Representatives


- If patient incompetent, the following have authority to direct healthcare under Idaho law:
 - Court-appointed guardian
 - Agent under durable power of attorney for healthcare
 - Spouse
 - Adult child
 - Parent
 - Person designated in delegation of parental authority
 - Other appropriate relative
 - Other person responsible for care

(IC 39-4504)

HOLLAND & HART 

Personal Representatives

- Not required to treat personal rep of minor (i.e., do not disclose protected info 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 rep as the patient is not in the best interest of patient, e.g., abuse.

HOLLAND & HART 

Disclosures to Family and Personal Representatives

- Potential bases for disclosure
 - Personal rep has right to access protected info.
 - 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 HIPAA exception.

HOLLAND & HART 

Business Associates (45 CFR 164.502 and .504)



HOLLAND & HART 

Business Associates

- May disclose PHI to business associate if you have valid business associate agreement.
 - Requires business associate to comply with certain HIPAA requirements.
 - Must contain required elements.
- Business associate = someone you want to create, maintain, transmit, or access PHI for you.

HOLLAND & HART 


Business Associates

<p><u>Business Associates</u></p> <ul style="list-style-type: none"> • Management company • Billing company • EMR / IT specialist • Consultant • Accountant • Attorney • Malpractice insurer • Interpreters • Data storage entities • Data transmission services if have routine access to info • Subcontractors of forgoing • Others 	<p><u>NOT Business Associates</u></p> <ul style="list-style-type: none"> • Workforce members, i.e., if you have right to control • Other providers when they are providing treatment • Members of organized healthcare arrangement • Insurance companies unless acting for you • Mere conduits of information, e.g., mailman • Janitors
---	---

HOLLAND & HART 

Business Associates


- Covered entity is liable for acts of business associate if:
 - Knew or should know that business associate is violating HIPAA and covered entity fails to act; or
 - Business associate is the covered entity’s agent.
- Make sure business associate is an independent contractor, not an agent.
 - Business associate agreement should confirm same.
 - Make sure you do not control method and manner of business associate’s functions.
- *But see recent settlements....*

HOLLAND & HART 

Business Associates

<p>North Memorial Health Care of Minnesota</p> <ul style="list-style-type: none"> • Theft of Accretive employee’s laptop containing PHI of 9,500 persons. • No BAA. • No risk analysis. • Paid \$1,550,000. 	<p>Raleigh Orthopedic Clinic</p> <ul style="list-style-type: none"> • Turned over x-rays to vendor who was to destroy films after extracting silver. • No BAA. • Paid \$750,000
--	---

- *But why impose penalties where business associate had independent obligation to comply with HIPAA?*
- *Does this create obligation to self-report disclosures absent BAAs?*

HOLLAND & HART 

HIPAA Security Rule (45 CFR 164.300 et seq.)



HOLLAND & HART 

NBC NEWS HOME TOP VIDEOS DECISION 2016 ON DEMAND PARIS TERROR ATTACKS SAN BERNARDINO SHOOTING

U.S. WORLD LOCAL POLICE HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATIONS SPORTS MORE

NIGHTLY NEWS TODAY MEET THE PRESS GATEWAY

NBC News (February 13, 2016)

- Healthcare related hacking up 11,000% since last year.
- 1/3 of Americans have had their health records compromised.
- Health records receive premium on “dark web”
 - ✓ Credit cards: \$1 to \$3
 - ✓ SSNs: \$15
 - ✓ Complete health records: \$60

Hacking of Health Care Records Skyrockets

by TOM COSTELLO

FEB 13 2016, 4:10 AM ET

A man types on a computer keyboard in the dark in this February 28, 2015 illustration. The picture: A barrage of damaging cyberattacks is shaking up the security industry, with some businesses and organizations no longer ensuring they can keep records of day, and instead turning to storing a portfolio and from within their networks. @NACFOR HEALTH - Reuters

For John Kuhn, a simple X-ray after a snowboarding accident turned into an accounting nightmare when the hospital billed him \$20,000 for a surgery he never had.

FOREVER

Anthem's big data breach is already sparking lawsuits

by Tom Huddleston, Jr. @thuddle




MedStar Georgetown University Hospital

HACKERS PARALYZED HOSPITAL CHAIN

ANEMO ACCO-FREE CAMPUS

HIPAA Security Rule

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



Protect ePHI:

- Confidentiality
- Integrity
- Availability

40 HOLLAND & HART LLP

Risk Analysis

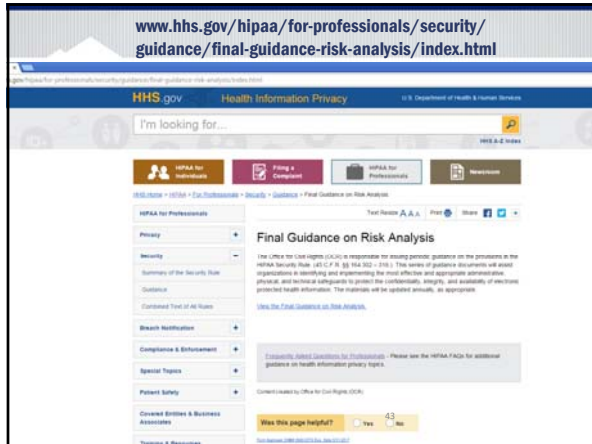
- Security rule requires that covered entities and business associates “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of [ePHI]...” (45 CFR 164.308(a)).
 - Frequently cited in recent violations.
- Periodically reevaluate analysis.
 - New systems or equipment.
 - Every few (very few?) years.
 - Include mobile devices.

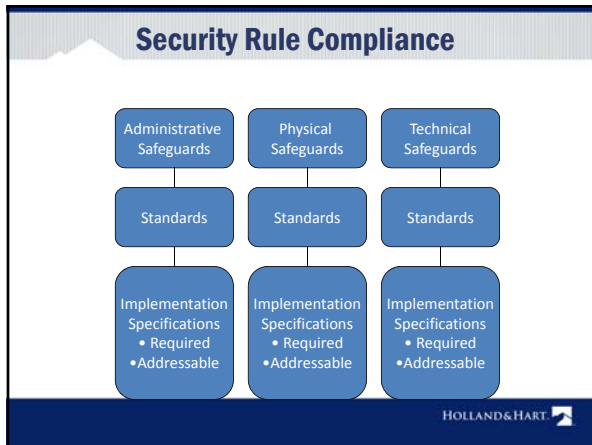
41 HOLLAND & HART LLP

www.healthit.gov/providers-professionals/security-risk-assessment-tool



42





- ### Administrative Safeguards
1. Security management process
 2. Assigned security responsibility
 3. Workforce security
 4. Information access management
 5. Security awareness and training
 6. Security incident procedures
 7. Contingency plan
 8. Evaluation
 9. Business associate contracts
(45 CFR 164.308)

Physical Safeguards

1. Facility access controls
2. Workstation use
3. Workstation security
4. Device and media controls

(45 CFR 164.310)

HOLLAND & HART LLP

Technical Safeguards

1. Access controls
2. Audit controls
3. Integrity of e-PHI
4. Person or entity authorization
5. Transmission security

(45 CFR 164.312)

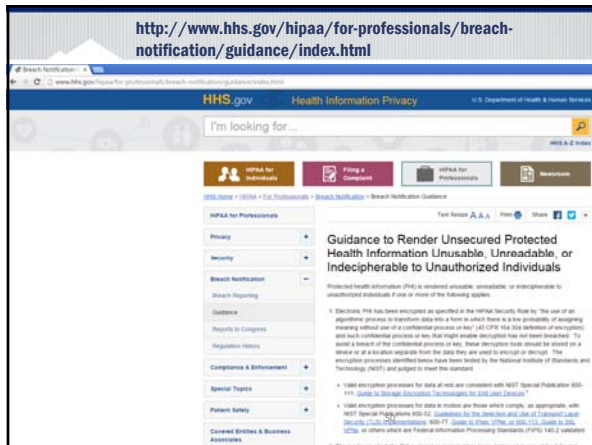
HOLLAND & HART LLP

Encryption

- Encryption is an addressable standard per 45 CFR 164.312:
 - (e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.
 - (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
- ePHI that is properly encrypted is “secured”.
 - Not subject to breach reporting.
- OCR presumes that loss of unencrypted laptop, USB, mobile device is breach.


HOLLAND & HART

<http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>



The screenshot shows the HHS.gov website with a search bar and navigation tabs for 'HIPAA for Professionals', 'Filing a Complaint', and 'HIPAA for Professionals'. The main content area displays the title 'Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals' and provides detailed information about encryption standards and breach reporting requirements.


Beware Social Media, E-mail and Texts!



HOLLAND & HART

E-mails and Texts

- 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)

HOLLAND & HART 

HealthIT.gov

Providers & Professionals

Can you use texting to communicate health information, even if it is to another provider or professional?

? Can you use texting to communicate health information, even if it is to another provider or professional?


a It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages.

However, your organization may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices. Read more about the five steps organizations can take to manage mobile devices when they are used by health care providers and professionals.

E-mails and Texts

Can you use texting to communicate health information, even if it is to another provider or professional?

Answer: It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages. However, your organization may approve texting after performing a risk analysis or implementing a third-party messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices. Read more about the five steps organizations can take to manage mobile devices when they are used by health care providers and professionals. (HealthIT.gov FAQ)

HOLLAND & HART 










Security Rule: Documentation

- Implement written policies and procedures to comply with standards and specs.
- Maintain documentation in written or electronic form.
- Required
 - Maintain for 6 years from later of creation or last effective date.
 - Make documents available to persons responsible for implementing procedures.
 - Review and update documentation periodically.

59 HOLLAND & HART 

HIPAA Patient Rights (45 CFR 164.520-.528)



HOLLAND & HART 


Individual Rights

- Right to receive notice of privacy practices.
- Right to request additional restrictions on use or disclosure for treatment, payment or operations.
- Right to receive information by alternative means or at alternative location.
- Right to access protected health information.
- Right to request amendment of protected health information.
- Right to limited accounting of disclosures.

HOLLAND & HART 


Notice of Privacy Practices

- Notice summarizes HIPAA rules and explains how you will use the patient's information.
- 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.
- If you have not done so, should update notice to include requirements of HIPAA Omnibus Rule.
(45 CFR 164.520)

62 HOLLAND & HART 


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!
- 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)

HOLLAND & HART 

Restrictions on Disclosures to Health Insurers

- Per omnibus rule, must agree to request of a patient to restrict disclosure of protected info to a health plan if:
 - Protected info 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)

HOLLAND & HART 

Request Alternative Communications

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


(45 CFR 164.522(b))

HOLLAND & HART 

Access PHI

- Patient or personal rep generally has right to inspect and obtain copy of PHI in "designated record set, i.e., documents used to make decisions concerning healthcare or payment.
- Must respond within 30 days.
- Must provide records in requested form if readily producible, including electronic form.
- May require written request.
- May charge reasonable cost-based fee, i.e., cost of actual labor and materials in making copies, not administrative or retrieval fee.
- Check with privacy officer or review 45 CFR 164.524 before denying request.


(45 CFR 164.524)

HOLLAND & HART 

Accounting of Disclosures

- Individual may obtain accounting of certain disclosures made for prior 6 years.
 - Improper disclosures.
 - Disclosures for certain safety or government functions under 45 CFR 164.512.
- ** Watch for new regulations.*
- Must maintain log of disclosures, including:
 - Date of disclosure.
 - Name of entity receiving disclosure.
 - Description of info disclosed.
 - Describe purpose of disclosure.
- Must account for disclosures by business associates.
- Check with privacy officer.

(45 CFR 164.528)

HOLLAND & HART 

Administrative Requirements (45 CFR 164.530)



HOLLAND & HART 

Administrative Requirements

- Designate privacy and security officers.
- Train workforce.
- Implement written policies and procedures.
- Respond to complaints and violations.
- Mitigate improper disclosures.
- Maintain documentation for 6 years.
- Implement reasonable safeguards.
 - “Incidental disclosures” do not violate HIPAA.

(45 CFR 164.530)

HOLLAND & HART 

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

(45 CFR 164.530(c))

73 HOLLAND & HART LLP

Reasonable Safeguards per OCR Guidance

<p>NOT required to:</p> <ul style="list-style-type: none"> • Remodel. • Eliminate sign-in sheets. • Isolate x-ray boards. • Remove bedside charts. • Buy a computer. 	<p>MAY be required to:</p> <ul style="list-style-type: none"> • 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.
--	--

74 HOLLAND & HART LLP

Breach Notification Rule





75 HOLLAND & HART LLP

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.)

76 HOLLAND & HART 

“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)


77 HOLLAND & HART 

“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)

78 HOLLAND & HART 

“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)


79 HOLLAND & HART 

Breach Notification

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.*

80 HOLLAND & HART 

Breach of Unsecured PHI


- 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.

81 HOLLAND & HART 

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.)


82 HOLLAND & HART 

Notice to Individual

- 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.


83 HOLLAND & HART 

Notice to Individual

Notice must contain:

- 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)).

84 HOLLAND & HART 

Notice to Individual

- **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))

85 HOLLAND & HART 

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))


86 HOLLAND & HART 

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>.**


87 HOLLAND & HART 

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.

91 HOLLAND & HART 

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)

92 HOLLAND & HART 

Action Items


HIPAA Top 10 List



HOLLAND & HART 


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.

HOLLAND & HART 


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

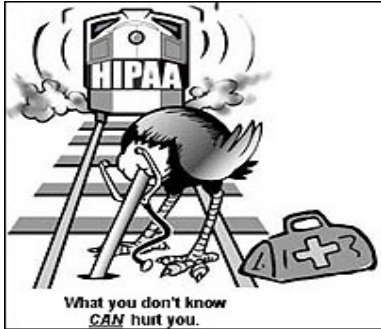
HOLLAND & HART 

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


HOLLAND & HART 

Do not do this...



Remember:

- Must mitigate
- No penalty if correct within 30 days
- Must give breach notice within 60 days

97 HOLLAND & HART 

Check on Insurance

- Check your 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.

98 HOLLAND & HART 

Additional Resources





HOLLAND & HART 



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 listserv**
 - Notice of HIPAA changes

101 



Kim C. Stanger
kcstanger@hollandhart.com
(208) 383-3913

HOLLAND&HART 