HIPAA Hot Topics

Kim C. Stanger
ISB Health Law Section
(6/16)

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.

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.

Recent Developments

- Recent enforcement actions.
- Private lawsuits.
- Cybersecurity threats.
- Liability for business associates' conduct.
- Phase 2 audits.
- Patient access guidance.
- Communicating via e-mail or text.

HIPAA: Recent Enforcement

Enforcement

- Civil penalties
  - $100 to $50,000 per violation
- Criminal penalties
  - $50,000 + 1 year to $250,000 + 5 years
- 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.

Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	• $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	• $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	• $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	• At least $50,000 per violation • Up to $1.5 million per type per year • Penalty is mandatory

(45 CFR 160.404)

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.

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

FOR IMMEDIATE RELEASE
January 2, 2013

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

HHS announces first HIPAA breach settlement involving less than 500 patients

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

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

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

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

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

A new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and*

HIPAA: Avoiding Civil Penalties

You can likely avoid HIPAA civil penalties if you:

- Have required policies and safeguards in place.
- Execute business associate agreements.
- Train personnel and document training.
- Respond immediately to mitigate and correct any violation.
- Timely report breaches if required.

No "willful neglect" = No penalties if correct violation within 30 days.

Private Lawsuits Based on HIPAA

HIPAA: Private Lawsuits

- No statutory private cause of action.
- But HIPAA violation may support state law tort clam.
  - Common law privacy torts
  - Negligence/malpractice
    - *Byrne v. Avery Center for Ob. and Gyn*, 2014 WL 5507439 (Conn. 11/11/14) ("to the extent it has become the common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services..., HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claim arising from allegations of negligence in...").
  - Negligence *per se*
    - *R.K. v. St. Mary's Medical Center,* 735 S.E.2d 715 (W.Va. 2012)

Anthem's big data breach is already sparking lawsuits

by Tom Huddleston, Jr. @tjhuddle FEBRUARY 6, 2015, 1:01 PM EST

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 l n July 26, a jury in Marion County, Indiana awarded $1.44 millior legations that the customer's pharmacist accessed, reviewe tion history with others who then used the information to intimi eart of the case was a tangled love triangle in which the pharmac antically involved with the customer, resulting in the birtl ed of the relationship, she allegedly accessed the custor ed it with her husband, who then used the information to intimi nanding child support payments.

The customer filed suit agains n Indiana Superior Court, claiming that both parties had breache s of confidentiality and privacy. The complaint also included c , and publication of private facts against the pharmacist and cl and retention against 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

Security Rule Compliance

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

NEWS
FEB 13 2016, 4:51 AM ET

Hacking of Health Care Records Skyrockets

by TOM COSTELLO

A man types on a computer keyboard in Warsaw in this February 28, 2013 illustration file picture. A barrage of damaging cyberattacks is shaking up the security industry, with some businesses and organisations no longer assuming they can keep hackers at bay, and instead turning to waging a guerrilla war from within their networks. KACPER PEMPEL / Reuters

SHARE
Share

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.

Tags: hacker | ransomware | hospitals | hostage | data

Hacker Ransomware Hits Hospitals, Holds Data Hostage

HIPAA Security Rule

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

Protect ePHI:

- Confidentiality
- Integrity
- Availability

Privacy and Security

Health Information Privacy, Security, and Your EHR

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

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

Cybersecure:

Your Medical Practice

Play the Game ›

Integrating Privacy & Security Into Your Medical Practice

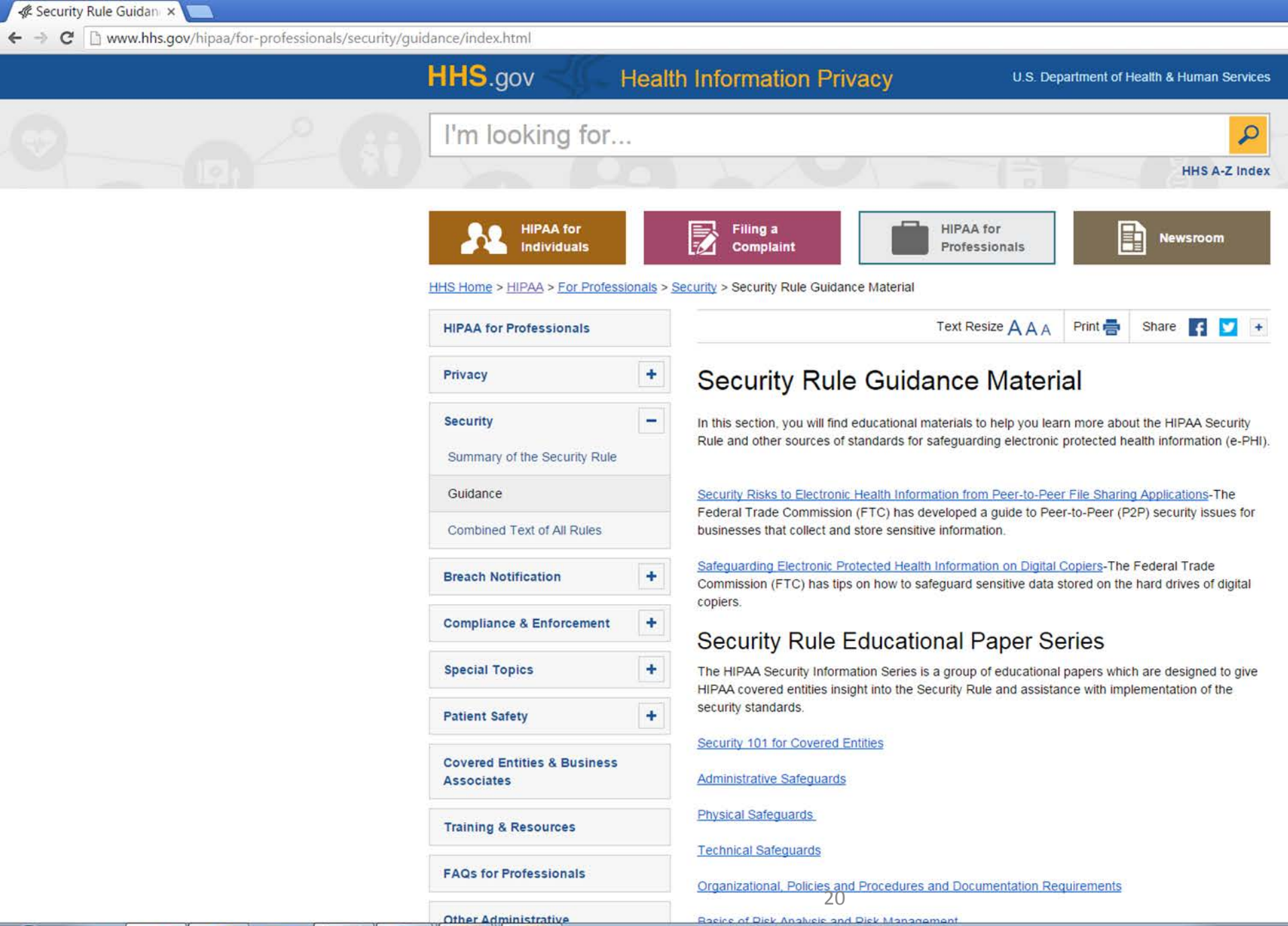
The HIPAA Privacy and Security Rules protect the privacy and security of e health

Privacy & Security 10 Step Plan

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

Privacy & Security and Meaningful Use

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


Security Rule Guidan
www.hhs.gov/hipaa/for-professionals/security/guidance/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 > For Professionals > Security > Security Rule Guidance Material
HIPAA for Professionals
Privacy
Security
Summary of the Security Rule
Guidance
Combined Text of All Rules
Breach Notification
Compliance & Enforcement
Special Topics
Patient Safety
Covered Entities & Business Associates
Training & Resources
FAQs for Professionals
Other Administrative
Text Resize A A A
Print
Share
Security Rule Guidance Material
In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).
Security Risks to Electronic Health Information from Peer-to-Peer File Sharing Applications-The Federal Trade Commission (FTC) has developed a guide to Peer-to-Peer (P2P) security issues for businesses that collect and store sensitive information.
Safeguarding Electronic Protected Health Information on Digital Copiers-The Federal Trade Commission (FTC) has tips on how to safeguard sensitive data stored on the hard drives of digital copiers.
Security Rule Educational Paper Series
The HIPAA Security Information Series is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards.
Security 101 for Covered Entities
Administrative Safeguards
Physical Safeguards
Technical Safeguards
Organizational, Policies and Procedures and Documentation Requirements
Basics of Risk Analysis and Risk Management

Other Cyberliability Laws

- Idaho Identity Theft Statute, IC 28-51-101 et seq.
  - Requires report of security breach.
  - $25,000 fine for failure to report
- Federal Trade Comm'n Act ("FTCA") § 5 (15 USC 45(a))
  - Prohibits unfair or deceptive acts affecting commerce.
    - Deceipt = 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.

LabMD, Inc., In the Matter of

TAGS: Health Care | Consumer Protection | Privacy and Security | Data Security

LAST UPDATED: FEBRUARY 5, 2016

In the Matter of LabMD, Inc., a corporation

FTC MATTER/FILE NUMBER: 102 3099

DOCKET NUMBER: 9357

RELATED CASE: LabMD, Inc. v. Federal Trade Commission

CASE SUMMARY

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.

Liability for Business Associates

Business Associates

- HIPAA applies directly to business associates.
  - Create, receive, maintain, or transmit protected health info ("PHI") on behalf of covered entity.
  - Business associates must comply with:
    - Business associate agreement ("BAA").
    - Security rule.
    - Breach notification rule.
- Covered entity may disclose PHI to business associate if have valid BAA.

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.
    - Under federal common law of agency.
    - Depends on facts, not characterization.
- But see recent settlements…

Business Associates

North Memorial Health Care of Minnesota

- Theft of Accretive employee's laptop containing PHI of 9,500 persons.
- No BAA.
- No risk analysis.
- Paid $1,550,000.

Raleigh Orthopedic Clinic

- 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?*

HIPAA Phase 2 Audits

HIPAA for Professionals

Privacy +

Security +

Breach Notification +

Compliance & Enforcement −

Enforcement Rule
Enforcement Process
Enforcement Data
Resolution Agreements
Case Examples
Audit
Reports to Congress
State Attorneys General

Audit Protocol – Updated April 2016

The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule. The audit protocol is organized by Rule and regulatory provision and addresses separately the elements of privacy, security, and breach notification. The audits performed assess entity compliance with selected requirements and may vary based on the type of covered entity or business associate selected for review. You may submit feedback about the audit protocol to OCR at OSOCRAudit@hhs.gov.

The protocol is available for public review and searchable by keyword(s) in the table below; export options will be made available soon.

General Instructions:

1. Where the document says "entity," it means both covered entities and business associates unless identified as one or the other;

2. *Management* refers to the appropriate privacy, security, and breach notification official(s) or person(s) designated by the covered entity or business associate for the implementation of policies and procedures and other standards;

3. Entities must provide only the specified documents, not compendiums of all entity policies of

HIPAA Phase 2 Audits

- OCR collecting info for audit pool.
  - Failure to respond may result in entity being selected for audit or subject to a compliance review.
- Will conduct 200+ audits.
  - "Broad spectrum" of providers, health plans, clearinghouses, and business associates.
  - Primarily for education, training, to identify common problems so that OCR may provide guidance, and to help OCR develop future audit protocols.
  - BUT OCR reserves right to take enforcement action in the case of serious breaches.

HIPAA Phase 2 Audits

- Desk audit process
  - Request to submit documents within 10 business days.
  - Auditors will review and respond with findings.
  - Auditees will have 10 business days to review and return written comments.
  - Auditor will complete final audit report within 30 days.
- Onsite audit process
  - Notice of audit.
  - Entrance conference.
  - Audit occurs over 3 to 5 days.
  - Auditee will have 10 business days to respond to draft audit.
  - Auditor will complete final audit report within 30 days.

Patient Access to PHI

Access to Info

- Cignet Health Center fined $4,300,000.
  - $1,300,000: Failed to respond to 41 patients' requests to access info.
  - $3,000,000: Failed to cooperate with OCR's investigation.
  - Actions = "willful neglect" under new penalty structure.

www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

New OCR Guidance re Access

OCR Guidance on Access

- Individual and personal representative generally have a right to inspect and/or obtain a copy of protected health info in their designated record set, subject to certain exceptions. (45 CFR 164.524)
  - Includes info received from other providers.
  - Must provide in manner, form and format requested if readily producible.
  - "It is expected" that covered entities have capability to e-mail records.
  - May require individual to request access/copy in writing.
  - May not impose unreasonable barriers to access (e.g., pick up documents in person; access through portal; etc.)
  - May not require individual to provide reason for accessing info.
  - Have 30 days to respond, but encouraged to respond ASAP.

OCR Guidance on Access

- May deny access in limited circumstances. (45 CFR 164.524)
  - Unreviewable grounds for denial.
    - psych notes or info compiled in anticipation of litigation.
    - info obtained from someone other than a provider under promise of confidentiality.
  - Reviewable grounds for denial.
    - Access reasonably likely to endanger life or physical safety of someone.
    - Does NOT extend to concerns about psychological or emotional harm (e.g., concerns that individual will not be able to understand the info or may be upset by it).

OCR Guidance on Access

- May charge a reasonable cost-based fee, although OCR states that entities "should" provide copies free of charge.
  - labor for copying, scanning paper into electronic form, or uploading info after info is ready for copying , scanning, or uploading.
  - supplies for creating paper (e.g., paper, toner) or electronic copy (e.g., CD, USB).
  - postage.
  - preparation of explanation or summary, if individual agrees.
- May not charge for costs of reviewing, verifying, searching, retrieving info, maintaining systems, recouping capital for data access, or other costs.
- May not charge individual to access info.
- Must notify individual of approximate costs in advance when the manner, form and format are being discussed.
- "Should" post costs on website.
- "Should breakdown costs if requested by individual.

OCR Guidance on Access

- Must verify identity/authority of person making the request. (45 CFR 164.514(h))
  - If provide access through web portal, include authentication controls.

OCR Guidance on Access

- Individual or personal representative has right to direct that a copy of the record be transmitted to a third party. (45 CFR 164.524).
  - 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.

E-mailing and Texting

E-mailing and Texting

hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/

Tools Help

Kickback Statute | CMS home | CMS Stark | eCFR | EMTALA guidelines | Gmail | HH Secure | HIPAA (160) | HIPAA | Hotmail | Idaho Statutes | Page | Safet

HHS.gov

U.S. Department of Health & Human Services

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

HHS Home > HIPAA > For Professionals > FAQ > 2006-Does the Security Rule allow for sending e-PHI in an email or over the Internet

- Authorizations (30)
- Business Associates (33)
- Compliance Dates (5)
- Covered Entities (17)
- Decedents (8)
- Disclosures for Law Enforcement Purposes (7)
- Disclosures for Rule Enforcement (2)
- Disclosures in Emergency Situations (2)
- Disclosures Required by Law (6)
- Disclosures to Family and Friends (27)
- Disposal of Protected Health Information (6)
- Facility Directories (7)
- Family Medical History Information (3)
- FERPA and HIPAA (10)
- Group Health Plans (2)
- Health Information Technology (35)
- Incidental Uses and Disclosures (10)

Text Resize A A A | Print | Share

Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?

Answer:

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

Content created by Office for Civil Rights (OCR)

top

E-mail and Texting

Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?

Answer: The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

(OCR FAQ)

E-mailing and Texting

- HIPAA Privacy Rule allows patient to request communications by alternative means or at alternative locations.
  - Including unencrypted e-mail.

(45 CFR 164.522(b))

- Omnibus Rule commentary states that covered entity or business associate may communicate with patient via unsecured e-mail so long as they warn patient of risks and patient elects to communicate via unsecured e-mail to text.

(78 FR 5634)

- Does not apply to communications between providers.

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-mailing and Texting

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)

www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

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

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

HealthIT.gov

in Partnership with the National Learning Consortium

Newsroom | FAQs | Multimedia | Implementation Resources

Providers & Professionals | Patients & Families | Policy Researchers & Implementers

Benefits of EHRs | How to Implement EHRs | Privacy & Security | EHR Incentives & Certification | Success Stories & Case Studies | Resource Center

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

Print | Share

Privacy & Security

Your Mobile Device and Health Information Privacy and Security

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

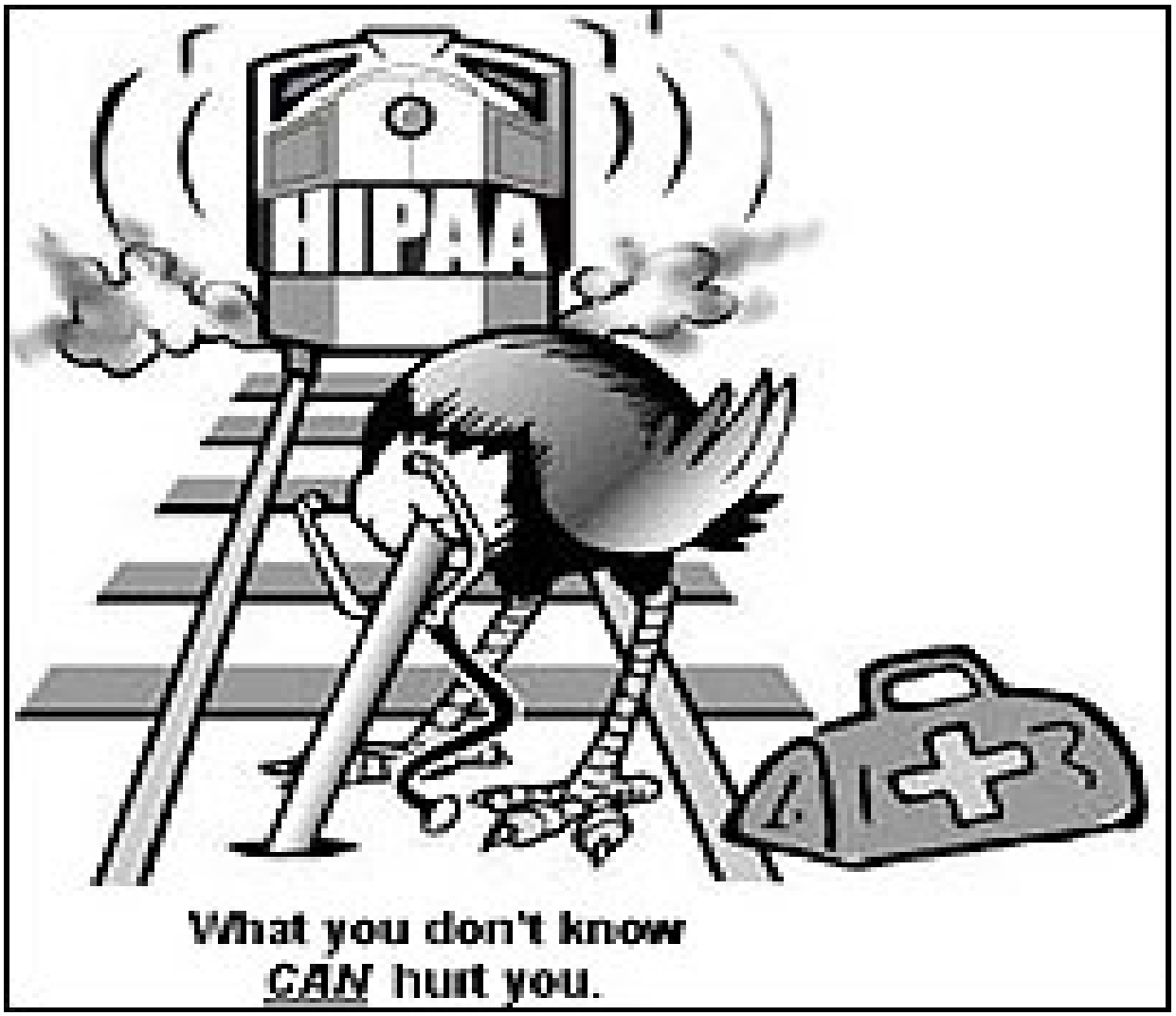
Read and Learn

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

Watch and Learn

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

Do not do this…



Remember:

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