HIPAA Privacy and Security Rules: Training for Covered Entities

Kim C. Stanger

(2-16)

HOLLAND&HART

This presentation is similar to any other seminar designed to provide general information on pertinent legal topics. The statements made and any materials distributed as part of this 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 speakers. 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 the law to your activities, you should seek the advice of your legal counsel.

Overview

- We'll discuss:
  - Why you should care about HIPAA
  - Privacy rules
  - Security rules
  - Patient rights
  - Breach notification
- This is an overview of the more significant rules.
- Staff: check with your privacy officer if you have questions.
- Privacy officers: know the regulations and your own state law.

Preliminaries

- Written materials
  - .ppt presentations
  - Article, *Complying With HIPAA: A Checklist for Covered Entities*
  - Sample Notice of Privacy Practices
- 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.

HOLLAND&HART

Health Insurance Portability and Accountability Act ("HIPAA")

- 45 CFR 164
  - .500: Privacy Rule
  - .300: Security Rule
  - .400: Breach Notification Rule
- HITECH Act
  - Modified HIPAA
  - Implemented by HIPAA Omnibus Rule

Remember Other Privacy Laws!

- Must comply with other law if it is more strict than HIPAA, i.e.,
  - Provides greater protection to patient info, or
  - Provides patients greater rights regarding their info.
- For example:
  - Medical Practices Act
  - Licensing regulations
  - Accreditation standards
  - Ethics standards
  - Common law duty

So, what's the big deal?!

- How would you feel if:
  - Staff at your doctor's office gossiped about your medical condition?
  - Your doctor's office posted your medical info on Facebook?
  - Your doctor shared your medical info with your employer?
  - The local hospital lost a laptop containing your unencrypted info, including
    - Your social security number?
    - Your account info?
    - Your insurance info?
    - Your medical info?

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 in 2015

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

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	• $50,000 fine • 1 year in prison
Committed under false pretenses	• 100,000 fine • 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	• $250,000 fine • 10 years in prison

(42 USC 1320d-6(a))

Criminal Penalties

- Physician and two hospital employees improperly accessed murdered newscaster's medical info.
- Convictions:
  - Physician: $5000 fine + 1 year probation
  - Employee 1: $2,500 fine + 1 year probation
  - Employee 2: $1,500 fine + 1 year probation

Additional Reasons to Comply

- State attorney general can bring lawsuit.
  - $25,000 fine per violation + fees and costs.
- Under HITECH, patients may recover % of fines.
  - Waiting for final rules.
- Patients can probably bring lawsuit.
- Must impose employee sanctions.
- HHS is conducting audits.
- Must self-report breach of unsecured protected health info.
  - Affected individuals
  - HHS
  - Sometimes local media

It's better to simply comply.

Who and What Does it Cover?

HOLLAND&HART

Covered Entities

- 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

Protected Health Information ("PHI")

- Individually identifiable health info, i.e., info that could be used to identify individual.
  - Name, fact that person is patient, etc.
  - Other info that may identify individual.
- Concerns physical or mental health, health care, or payment.
- Created or received by covered entity.
- Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.

Covered Actions

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

Use and Disclosure Rules

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 in patient's 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 govt purposes listed in 45 CFR 164.512.
  - Have a valid written authorization signed by patient that complies with 45 CFR 164.508.

(45 CFR 164.502-.512)

Treatment, Payment or Operations

- Consent is implied if use or disclosure is for—
  - Treatment
  - Payment
  - Health care operations
- Patient's authorization is not necessary.
  - Exception: 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)

Persons Involved in Care

- May use or disclose info 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 info to scope of person's involvement.
- Applies to disclosures after the patient is deceased.

(45 CFR 164.510)

Safety and Govt Functions

- Authorization is not required for certain govt or safety purposes so long as 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

(45 CFR 164.512)

- Check with privacy officer or 42 CFR 164.512 to determine if conditions are satisfied.

Authorization

- May use or disclose info 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.

(45 CFR 164.508)

Disclosure Optional

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

(45 CFR 164.502)

Verification

- Before disclosing PHI:
  - Verify the identity and authority of person requesting info if he/she is not known.
    - E.g., 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 164.514(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, .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))

Personal Representatives

- Not required to treat personal rep as patient (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.

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.

Business Associates

(45 CFR 164.502, .504)

HOLLAND&HART

Business Associates

- May disclose PHI to business associate if have valid business associate agreement ("BAA").
  - BAA requires business associate to comply with certain HIPAA requirements.
  - BAA must contain required elements.

- Business associate = someone you want to create, maintain, or access PHI for you.

Business Associates

Business Associates

- 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

NOT Business Associates

- 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

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.

HIPAA Security Rule

(45 CFR 164.300 et seq.)

HOLLAND&HART

Remember…

HOLLAND&HART

Security Rule Compliance

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

Intended to ensure:

- Confidentiality
- Integrity
- Availability

of ePHI.

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.

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

Security Risk Assessm ×

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

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 › Security Risk Assessment › Security Risk Assessment Tool

Print | Share

Security Risk Assessment

- Guide to Privacy and Security of Electronic Health Information
- Health IT Privacy and Security Resources
- Mobile Device Privacy and Security
- Model Notices of Privacy Practices
- Patient Consent for eHIE
- Privacy & Security Training Games
- Cybersecurity
- Security Risk Assessment
  - Security Risk Assessment Tool
  - Security Risk

Security Risk Assessment Tool

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool [.exe - 69 MB] to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

We understand that users with Windows 8.1 Operating Systems may experience difficulties downloading the SRA Tool, we are working to resolve the issue and will post here when a resolution is identified and implemented.

The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS's for desktop and laptop computers and Apple's iOS for iPad only. The iOS SRA Tool application for iPad

Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds.

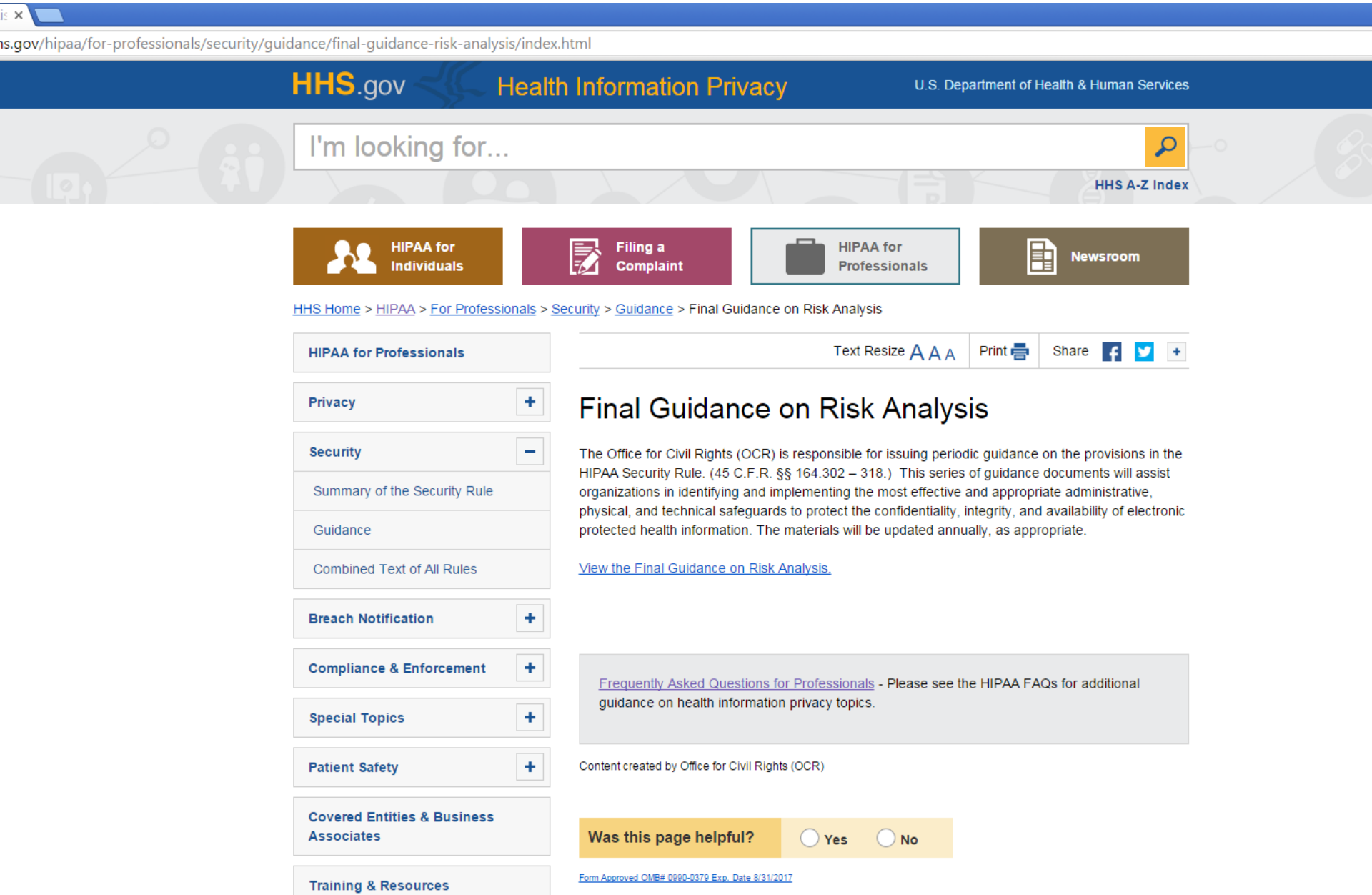
Read the top 10 list distinguishing fact from fiction.

SRA Tool (Windows version)

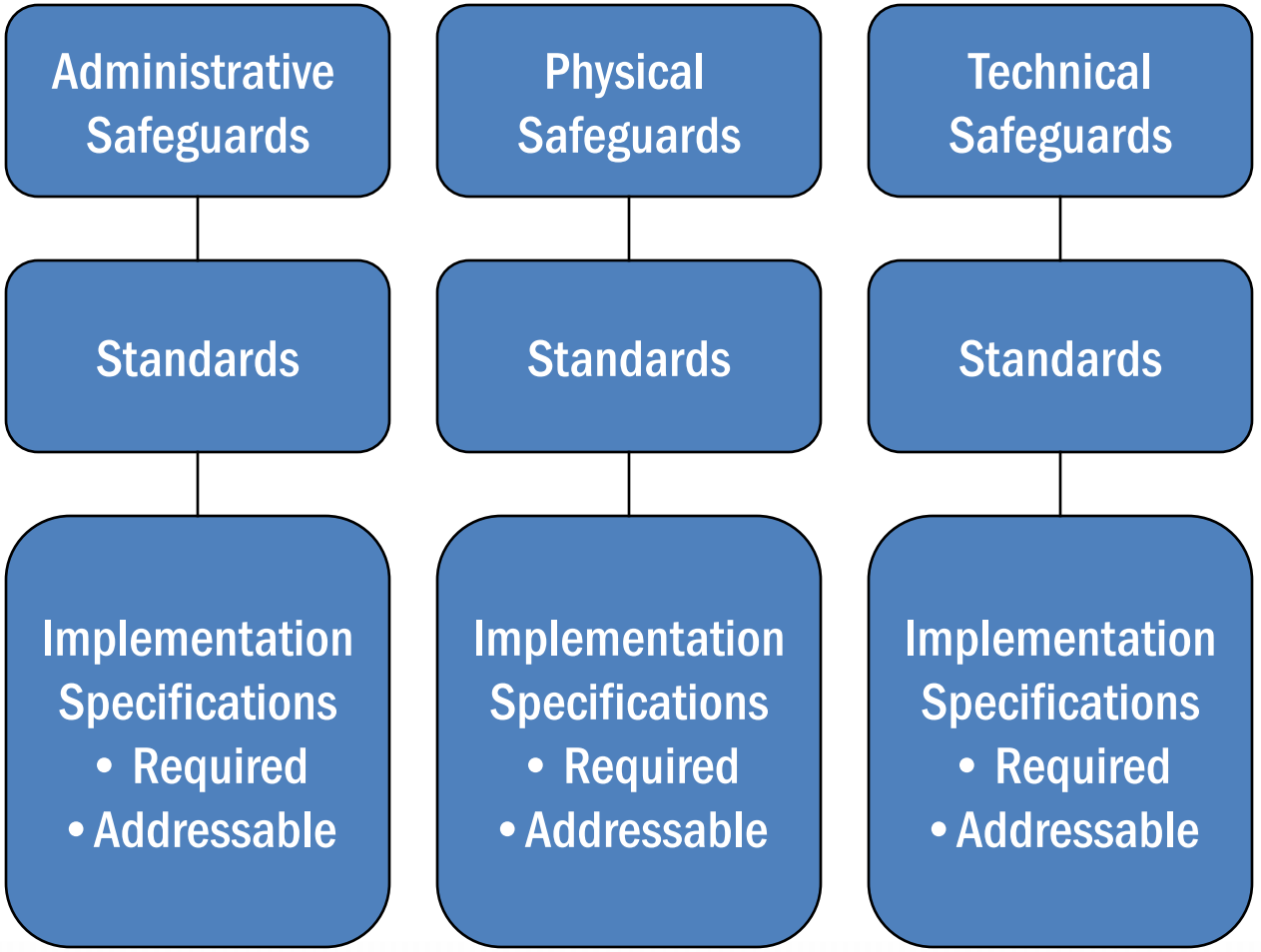
Download Tool ›

SRA Tool (iPad version)

www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html



Security Rule: Safeguards



Implementation Specifications

- "Required": implement the specification.
- "Addressable":
  - Assess reasonableness of specification.
  - If spec is reasonable, implement it.
  - If spec is not reasonable,
    - Document why it is not reasonable (e.g., size, cost, risk factors, etc.), and
    - Implement alternative if reasonable.
- Must review and modify as needed.

Security Rule: Safeguards

- Not technologically specific to accommodate technological advances.
- May use measures that reasonably allow you to comply with standards considering:
  - Size, complexity and capabilities,
  - Technical infrastructure, hardware and software,
  - Costs,
  - Probability and criticality of risks.

Security Rule: Administrative Safeguards

- Assign security officer.
- Implement policies, procedures and safeguards to minimize risks.
- Sanction workforce members who violate policies.
- Process for authorizing or terminating access to e-PHI.
- Train workforce members on security requirements.
- Process for responding to security incidents.
- Review or audit information system activity.
- Establish backup plans, disaster recovery plans, etc.
- Periodically evaluate security measures.

(45 CFR 164.308)

Security Rule: Physical Safeguards

- Limit access to physical facilities and devices containing e-PHI.
- Document repairs and modifications to facilities.
- Secure workstations.
- Implement policies concerning proper use of workstations.
- Implement policies concerning the flow of e-PHI into and out of the facility.
- Implement policies for disposal of e-PHI.
- Create a backup copy of e-PHI.

(45 CFR 164.310)

Security Rule: Technical Safeguards

- Assign unique names or numbers to track users.
- Implement automatic logoff process.
- Use encryption and decryption, where appropriate.
- Implement systems to audit use of e-PHI.
- Implement safeguards to protect e-PHI from alteration or destruction.
- Implement methods to ensure e-PHI has not been altered or destroyed.
- Implement verification process.
- Protect data during transmission.

(45 CFR 164.312)

www.healthit.gov/providers-professionals/ehr-privacy-security

Learn more about to

https://www.healthit.gov/providers-professionals/ehr-privacy-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 and Security

Print | Share

Privacy and Security

Health Information Privacy, Security, and Your EHR

If your patients lack trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you. Withholding their health information could have life-threatening consequences. To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure.

Your practice, not your EHR developer, is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR system.

Cybersecure:

Your Medical Practice

Play the Game ›

Integrating Privacy & Security Into Your Medical Practice

Security Risk Assessment

Privacy & Security and Meaningful Use

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.

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

Communicating by E-mail or Text

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

(45 CFR 164.522(b)).

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

(78 FR 5634)

www.healthit.gov/providers-professionals/ehr-privacy-security/10-step-plan

roviders-professionals/ehr-privacy-security/10-step-plan

Privacy & Security

Integrating Privacy & Security Into Your Medical Practice

Health Information Privacy and Security: A 10 Step Plan

Health IT Privacy and Security Resources

Mobile Device Privacy and Security

Model Notices of Privacy Practices

Patient Consent for eHIE

Privacy & Security Training Games

Cybersecurity

Security Risk Assessment

Health Information Privacy and Security: A 10 Step Plan

Before you get started, identify potential assistance from your regional extension center (REC) about where you can get help beyond the Privacy & Security resources.

Work with your EHR vendor(s) to let them know that protecting patient health information and meeting your HIPAA privacy and security responsibilities regarding electronic health information in your EHR is one of your major goals. Involve your practice staff and any other partners that you have to help streamline this process.

For an overview of specific Meaningful Use Requirements regarding EHR privacy and security, download Chapter Two of the Guide to Privacy and Security of Health Information [PDF - 1.5 MB].

For an overview of HIPAA privacy and security requirements visit HHS OCR's website.

Start your 10 steps at least 90 days before the day you target to start the EHR incentive program.

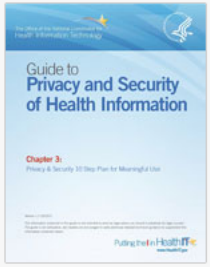
Preparation

1. Confirm you are a "Covered Entity"

Most health care providers are covered entities, and thus, have HIPAA responsibilities for individually identifiable health information. Use this HHS tool to confirm you are a covered entity.

2. Provide Leadership

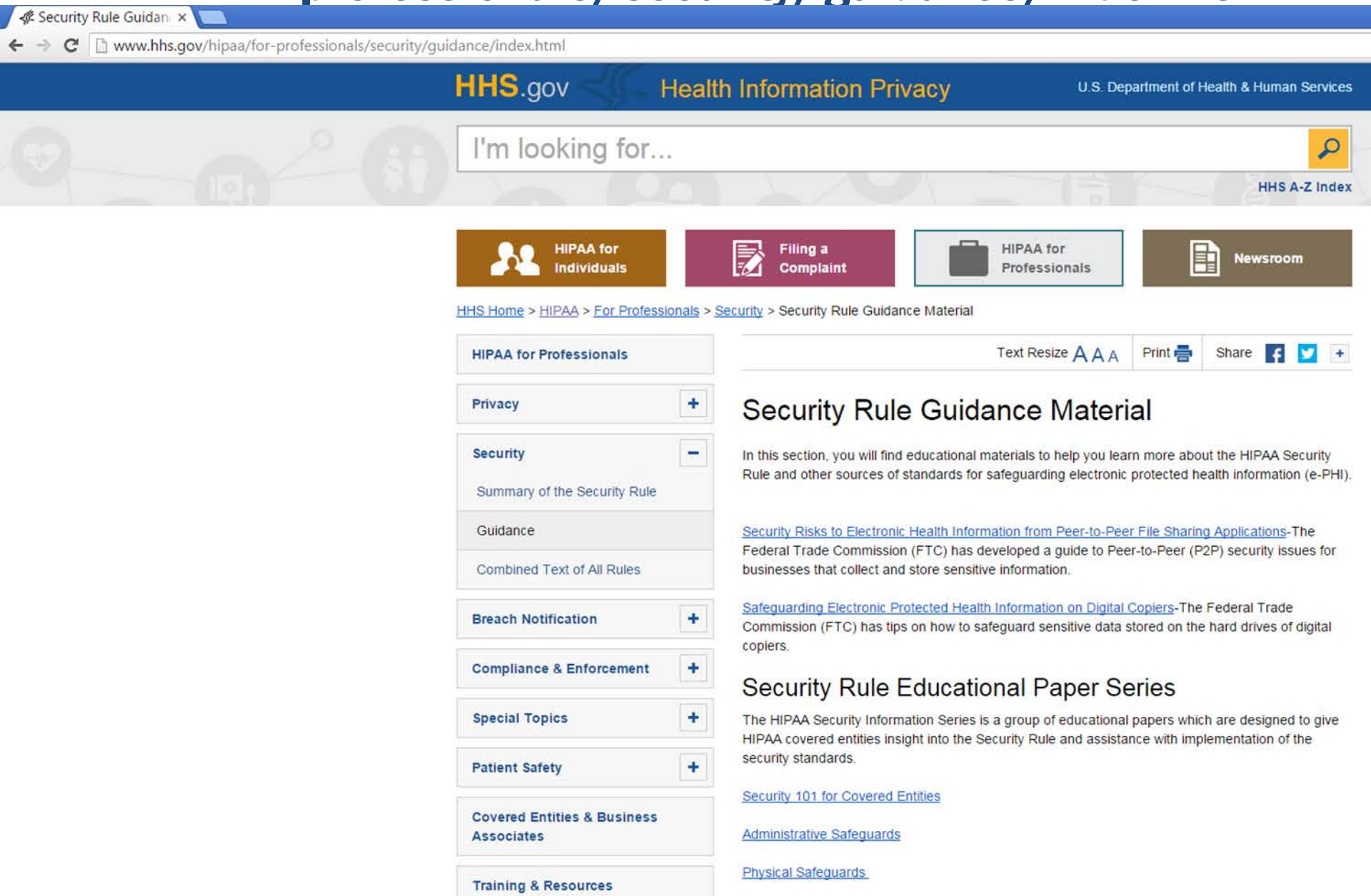
Your leadership—especially emphasizing the importance of protecting patient



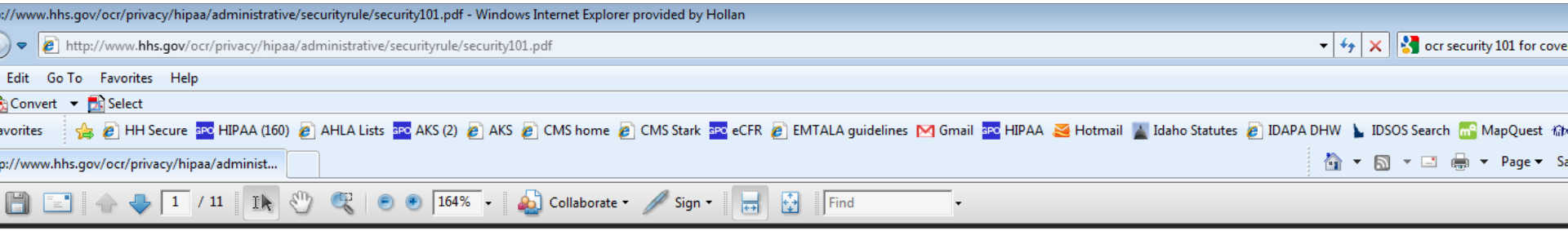
[PDF - 1.25 MB]

Download the Privacy

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



OCR Security Series



DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

HIPAA Security SERIES

Security Topics

☆1. Security 101 for

1 Security 101 for Covered Entities

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for

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

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.

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.

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)

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)

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)

Right to 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))

Right to Access Info

- Patient or personal rep generally has right to inspect and obtain copy of info in "designated record set, i.e., documents used to make decisions concerning healthcare or payment.
- Patient may direct that info be sent to another entity.
- 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 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

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

New OCR Guidance re Access

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.

Right to Request Amendment

- Individual has right to request amendment.
- Covered entity may deny request if:
  - Record not part of designated record set.
  - Entity did not create record unless creator not available.
  - Record is accurate and complete.
- Must act on request within 60 days.
- If accept request, amend record accordingly.
- If deny request, notify patient of basis for denial.
  - Patient has right to have request become part of record.
- Check with privacy officer or review 45 CFR 164.526 when responding to requests.

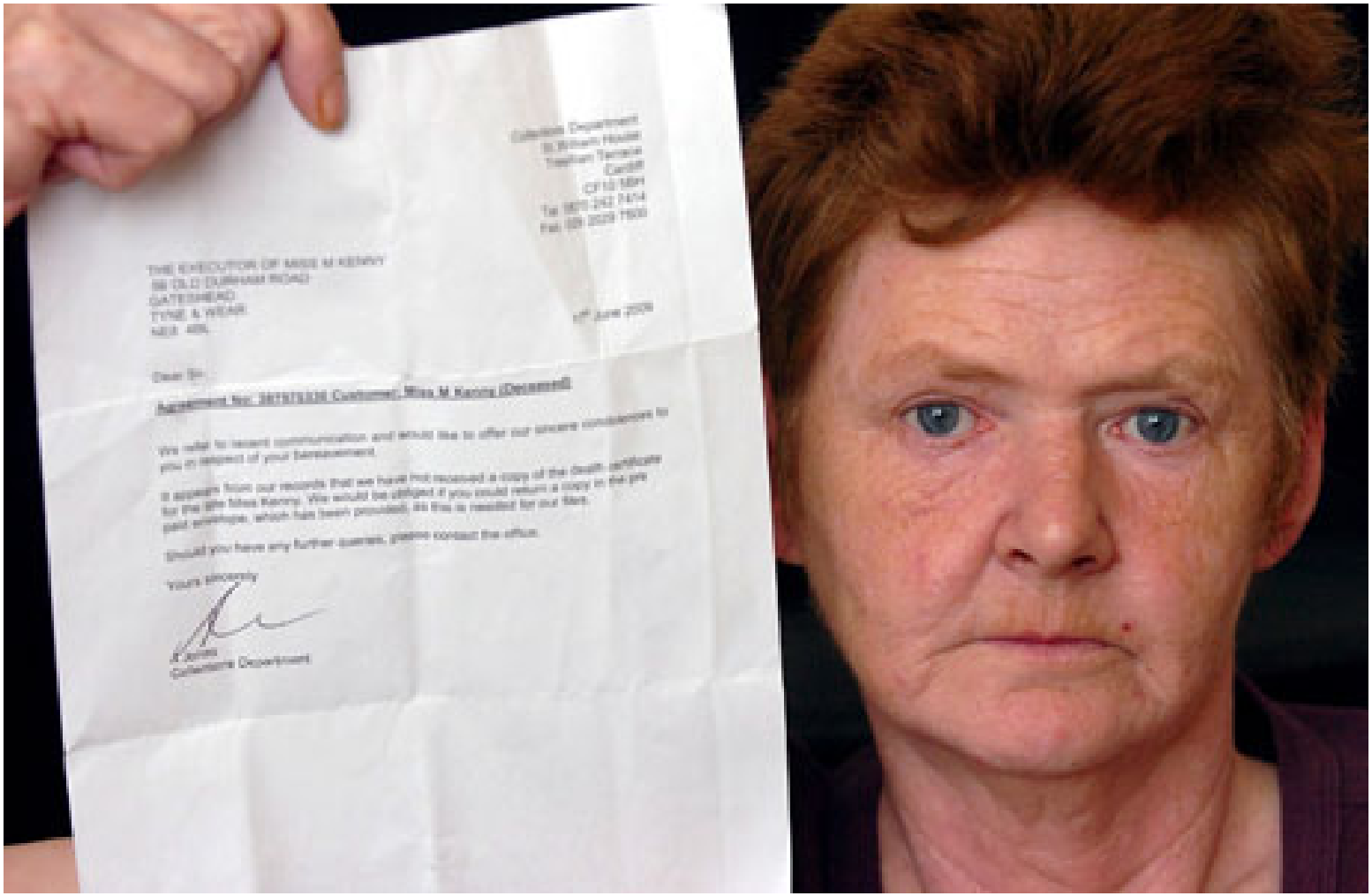
(45 CFR 164.526)

Right to Accounting of Disclosures

- Individual may obtain accounting of certain disclosures made during prior 6 years.
  - Improper disclosures.
  - Disclosures per 45 CFR 164.512.
- 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)

Breach Notification



(45 CFR 164.500 et seq.)

Breach Notification

- If there is breach of unsecured protected health info,
  - Covered entity must notify:
    - Each individual whose unsecured info has been or reasonably believed to have been accessed, acquired, used, or disclosed.
    - HHS.
    - Media, under certain circumstances.
  - Business associate must notify covered entity.

(45 CFR 164.400 et seq.)

Breach

- Acquisition, access, use or disclosure of protected health info 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)

Responding to Breaches

- *We'll discuss more about this in our webinar on February 18.*

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.

(45 CFR 164.530)

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))

Reasonable Safeguards per OCR Guidance

NOT required to:

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

MAY be required to:

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

Action Items

HOLLAND&HART

Action Items: HIPAA Compliance

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.
   - *See Privacy and Security Checklists.*

HOLLAND&HART

Action Items: HIPAA Compliance

5. Develop and use compliant forms.
   - Authorization, privacy notice, patient requests, etc.
6. Execute BAAs with business associates.
   - 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.

Action Items: HIPAA Compliance

9. Respond immediately to any potential breach.
   - Immediately take appropriate steps to mitigate.
     - Retrieve info.
     - Obtain assurances of no further use or disclosure.
     - Warn of penalties of violations.
   - Investigate facts to determine if there was a 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

Additional Resources

http://www.hhs.gov/hipaa

v/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.

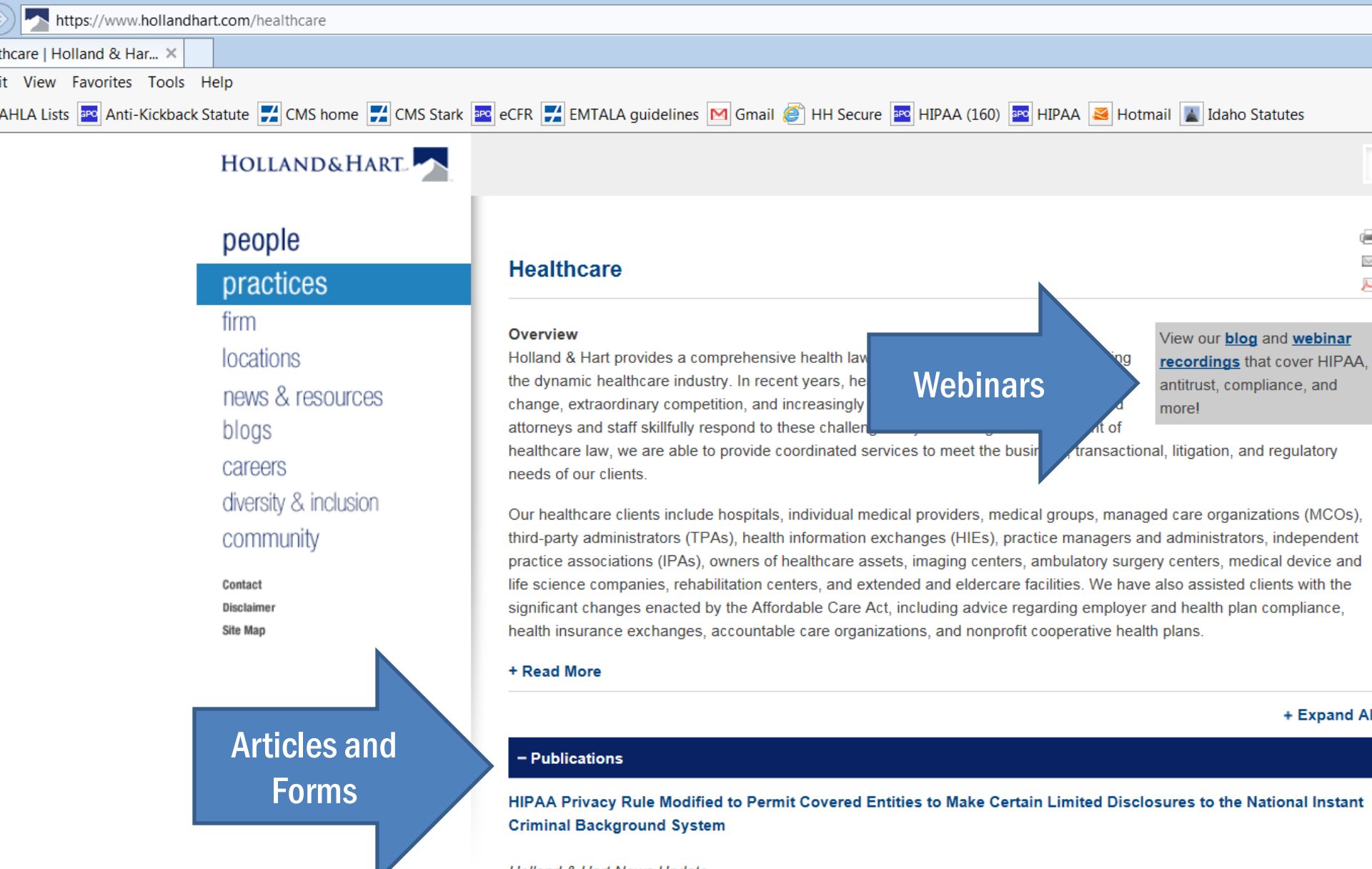
HIPAA Resources

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

Holland & Hart Resources

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

www.hollandhart.com/healthcare



Future Webinars

- *Health Law Basics* monthly webinar series
  - 2/11/16 HIPAA for Business Associates
  - 2/18/16 Responding to HIPAA Breaches
- *Healthcare Update* and *Health Law Blog*
  - Under "Publications" at www.hollandhart.com.
  - E-mail me at kcstanger@hollandhart.com.

HOLLAND&HART

Questions?

Kim C. Stanger

Holland & Hart LLP

(208) 383-3913

kcstanger@hollandhart.com