

HIPAA for Business Associates



February 11,
2015

Teresa D. Locke

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.

Overview

- Why should you care about HIPAA?
- Who are business associates?
- What must business associates do?
 - Business associate agreements.
 - Security Rule requirements.
 - Privacy Rule requirements.
 - Breach Notification Rule requirements.
- Liability for business associates and subcontractors.
- Additional resources.



Written Materials

- .ppt slides
- Sample Business Associate Agreement Provisions (<http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>).
- Kim Stanger publications on H&H website:
 - *HIPAA Update: Why and How You Must Comply.*
 - *Business Associate Decision Tree.*
 - *Checklist for Security Rules.*
 - *Complying with HIPAA: Checklist for Business Associate Agreements.*
 - *Avoiding Business Associate Agreements.*

Health Insurance Portability and Accountability Act, 42 CFR part 164

- HIPAA, not “HIPPA”



HIPAA History

- **HIPAA Privacy Rule (2003).**
 - Requires healthcare providers and health plans (“covered entities”) to protect the privacy of protected health info (“PHI”).
 - Execute business associate agreements (“BAA”) with business associates.
- **HIPAA Security Rule (2005).**
 - Requires covered entities to protect electronic PHI.
- **Health Info Technology for Economic and Clinical Health (“HITECH”) Act (2009).**
 - Required business associates to comply with HIPAA.
 - Strengthened HIPAA and penalties for violations.
- **HIPAA Omnibus Rules (enforced 9/23/13).**
 - Finalized and implemented HITECH Act.

Why you should care about HIPAA



HIPAA

**Business
Associates**

Covered Entities

Civil Penalties

(45 CFR 160.404)


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

Civil Penalties








- **Counting penalties**
 - If violation results in disclosure of info for multiple individuals, each individual is a separate violation.
 - E.g., loss of laptop containing 2000 names = 2000 violations.
 - If violation results from failure to implement required safeguard or policy, each day the safeguard or policy was not implemented is a separate violation.
 - E.g., if you failed to put in place safeguards and policies after 9/23/13, you are at 724 violations for each requirement violated and counting...

Civil Penalties

← →  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

 Case Examples and Resolut... x

File Edit View Favorites Tools Help

    Page ▾ Safety ▾ Tools ▾   

\$750,000	<ul style="list-style-type: none">• \$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies - August 31, 2015
\$218,400	<ul style="list-style-type: none">• HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications - June 10, 2015
\$125,000	<ul style="list-style-type: none">• HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records - April 22, 2015
\$150,000	<ul style="list-style-type: none">• HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software - December 2, 2014
\$800,000	<ul style="list-style-type: none">• \$800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014
\$4,800,000	<ul style="list-style-type: none">• Data Breach Results in \$4.8 Million HIPAA Settlements - May 7, 2014
\$1,725,220	<ul style="list-style-type: none">• Concentra Settles HIPAA Case for \$1,725,220 - April 22, 2014
\$250,000	<ul style="list-style-type: none">• QCA Settles HIPAA Case for \$250,000 - April 22, 2014
\$215,000	<ul style="list-style-type: none">• County Government Settles Potential HIPAA Violations - March 7, 2014
\$150,000	<ul style="list-style-type: none">• Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013
\$1,215,780	<ul style="list-style-type: none">• HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013
\$1,700,000	<ul style="list-style-type: none">• WellPoint Settles HIPAA Security Case for \$1,700,000 - July 11, 2013
\$275,000	<ul style="list-style-type: none">• Shasta Regional Medical Center Settles HIPAA Privacy Case for \$275,000 - June 13, 2013

Criminal Penalties

(42 USC 1320d-6(a))

- 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

Criminal Penalties

http://cdn.ca9.uscourts.gov/datastore/opinions/2012/05/10/10-50231.pdf - Windows Internet Explorer provided by Holland and Hart

http://cdn.ca9.uscourts.gov/datastore/opinions/2012/05/10/10-50231.pdf

Edit Go To Favorites Help

Convert Select

HH Secure HIPAA (160) AHLA Lists AKS (2) AKS CMS home CMS Stark eCFR EMTALA guidelines Gmail HIPAA Hotmail Idaho Statutes IDAPA DH

http://cdn.ca9.uscourts.gov/datastore/opinions/...

1 / 10 164% Collaborate Sign Find



FOR PUBLICATION

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

HUPING ZHOU,
Defendant-Appellant.

No. 10-50231

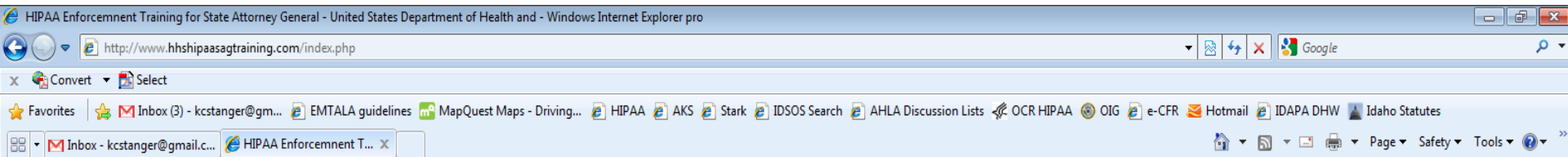
D.C. No.
2:08-cr-01356-
AJW-1

OPINION

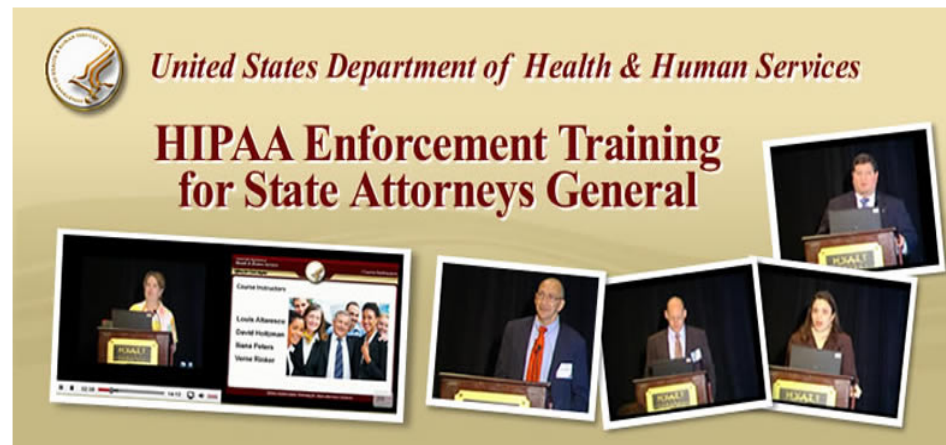
Appeal from the United States District Court
for the Central District of California
Andrew J. Wistrich, Magistrate Judge, Presiding

State Attorney General Lawsuits

- May sue for \$25,000 per violation + costs



- Agenda**
View Training Agenda
- Browse**
View All Presentations
- Speakers**
Browse Sessions by Presenters' Names
- Support**
View Frequently Asked Support Question



[Click Here to Start Course](#)

Business associate pays \$2.5 million

ATTORNEY GENERAL SWANSON SUES ACCRETIVE HEALTH FOR PATIENT PRIVACY VIOLATIONS

Debt Collector Lost Laptop Containing Sensitive Data on 23,500 Minnesota Patients

Minnesota Attorney General Lori Swanson today filed a lawsuit against Accretive Health, Inc., a debt collection agency that is part of a New York private equity fund conglomerate, for failing to protect the confidentiality of patient health care records and not disclosing to patients its extensive involvement in their health care through its role in managing the revenue and health care delivery systems at two Minnesota hospital systems.

Last July, Accretive lost a laptop computer containing unencrypted health data about 23,500 patients in Minnesota. The lawsuit alleges that Accretive gained access to sensitive patient data through contracts with the hospitals and numerically scored patients' risk of hospitalization and medical complexity, graded their "frailty," compiled per-patient profit and loss reports, and identified patients deemed to be "outliers."

"The debt collector found a way to essentially monetize portions of the revenue and health care delivery systems of some nonprofit hospitals for Wall Street investors, without the knowledge or consent of patients who have the right to know how their information is being used and to have it kept confidential," said Attorney General Swanson.

Attorney General Swanson added: "Accretive showcases its activities to Wall Street investors but hides them from Minnesota patients. Hospital patients should have at least the same amount of information about Accretive's extensive role in their health care that Wall Street investors do."

On July 25, 2011, an Accretive employee left an unencrypted laptop containing sensitive information on 23,500 Minnesota patients of two Minnesota hospital systems--Fairview Health Services and North Memorial Health Care--in a rental car after 10 p.m. in the parking area of the Seven Corners bar and restaurant district of Minneapolis. The laptop was stolen. The lawsuit includes a "screen shot" that Fairview sent to a Minnesota patient who requested to know the data about the patient that was on the laptop. The screen shot has personal identity information, such as the patient's name, address, date of birth, and Social Security number. It also includes a checklist to denote whether the patient has 22 different chronic medical conditions and, if so, the

Additional Reasons to Comply

- Unhappy clients.
- Clients may need to terminate services agreement.
- Individuals can probably bring lawsuit.
 - No private cause of action under HIPAA.
 - May claim HIPAA is the standard of care.
 - May sue for breach of business associate agreement.
- Must self-report breach of unsecured PHI.
 - Business associate must notify covered entity.
 - Covered entity must notify:
 - Affected individuals
 - HHS
 - Media, if breach involves over 500 persons.
- In future, affected individuals will be able to recover a percentage of fines or settlements.

Avoiding HIPAA Penalties

- The good news: covered entities and business associates may usually avoid civil penalties if they:
 - Implement required policies and safeguards.
 - See materials we have provided.
 - Train members of workforce and document training.
 - Use this program to train workforce.
 - Respond immediately to possible violation.
 - May mitigate any damage.
 - May avoid breach reporting obligation.
 - Affirmative defense if you do not act with willful neglect and correct violations within 30 days.

Whom and What Does it Cover?



Protected Health Info (“PHI”)

(45 CFR 160.103)

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

- NOT de-identified info.

Covered Entities

(45 CFR 160.103)

- 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.

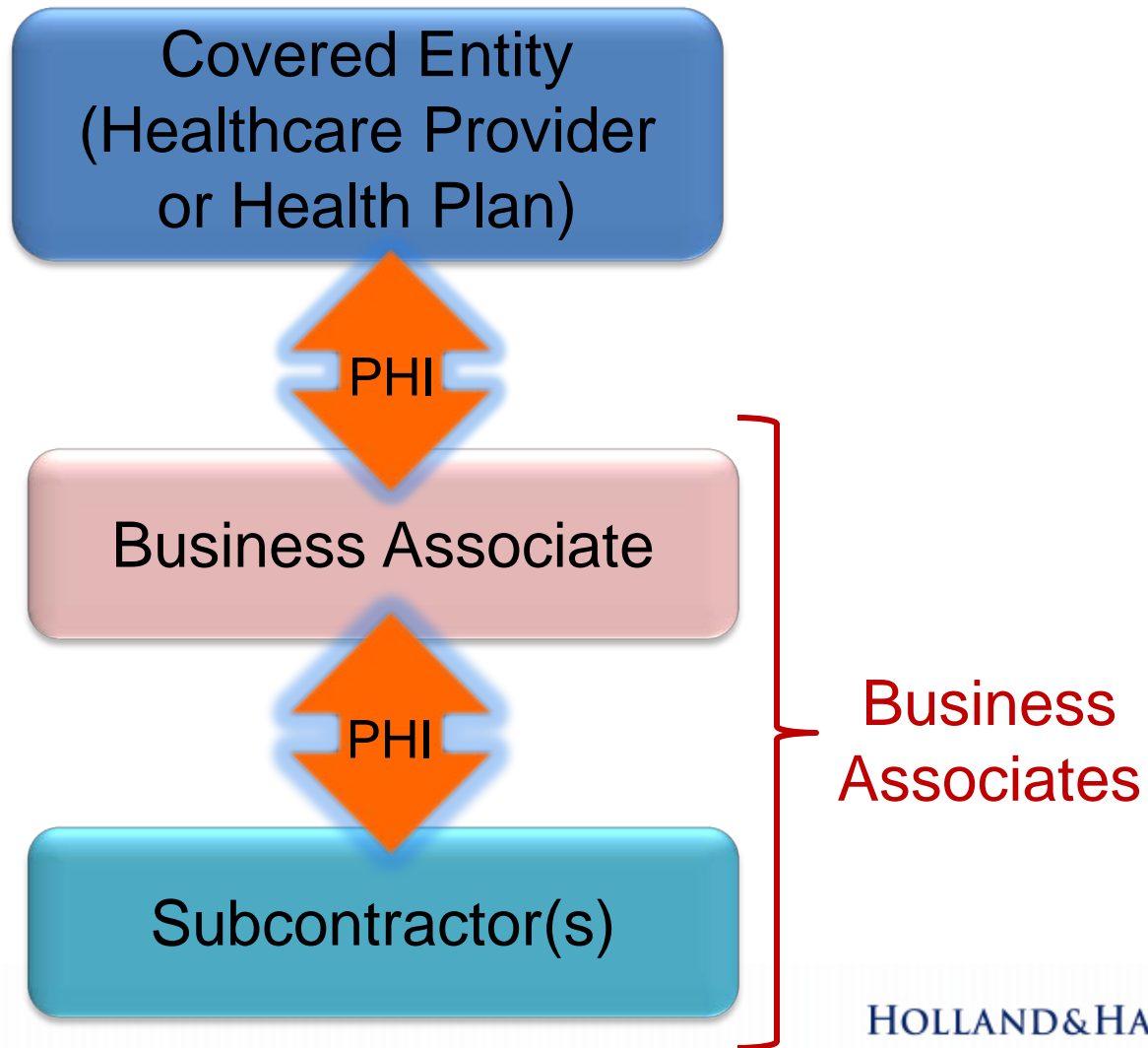
*The forgotten
HIPAA target*

Business Associates

(45 CFR 160.103)

- Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity to perform:
 - A function or activity regulated by HIPAA (e.g., healthcare operations, payment, covered entity function), or
 - Certain identified services (e.g., billing or claims management, legal, accounting, or consulting services).
 - Health information organizations and e-prescribing gateways.
 - Data transmission companies if they routinely access PHI.
 - Data storage companies (e.g., cloud computing, off-site storage facilities) even if they do not access PHI.
 - Patient safety organizations.
- Covered entities acting as business associates.
- Subcontractors of business associates.

Business Associates



Not Business Associates

- **Members of covered entity's workforce.**
 - Covered entity has control over the person.
- **Entities who do not handle PHI as part of their job duties.**
 - Janitor, mailman, some vendors, etc.
- **Entities that receive PHI to perform functions on their own behalf, not on behalf of covered entity.**
 - E.g., banks, third party payors, etc.
- **Other healthcare providers while providing treatment.**
- **Data transmission companies that do not routinely access PHI.**
 - Entity is mere “conduit” of PHI.
- **Maybe data storage companies that receive encrypted w/out the key.**
- **Members of an organized healthcare arrangement.**
 - Group of entities that provide coordinated care.

See Article, Avoiding BAAs

Business Associate Decision Tree

Will an outside entity ("Entity") provide services to or on behalf of the covered entity?

[Note: This does not apply to (1) an employee, volunteer, trainee, or other person whose conduct is under the direct control of the covered entity, (2) an entity who is performing functions as part of the covered entity's organized health care arrangement,¹ or (3) entities who receive info for their own purposes, and not to provide services to or on behalf of the covered entity (e.g., payors, government agencies, independent researchers, etc.).]

No

The Entity is not a business associate

Yes

Will the Entity create, receive, maintain or transmit PHI in the course of providing services to or on behalf of the covered entity?

[Note: This does not apply to entities who may incidentally see or hear PHI, but whose job duties for the covered entity do not involve the creation, receipt, maintenance, or transmission of PHI (e.g., a janitor, delivery person, or electrician who happens to be providing services in the building)].

No

The Entity is not a business associate

Yes

Is the Entity a healthcare provider who is receiving the PHI for purposes of treating the individual?

Yes

The Entity is not a business associate

No

Does the Entity provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity?

OR

Does the Entity provide claims processing or administration; data analysis, processing or administration; or utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing services for the covered entity?

OR

Is the Entity a health information organization, e-prescribing gateway, or other entity that provides data transmission services with respect to PHI and the entity requires access to the PHI on a routine access (i.e., the entity is not merely the conduit for the information)?

OR

Does the Entity offer a personal health record to one or more individuals on behalf of the covered entity?

No

The Entity is not a business associate

Yes

The Entity is a business associate. You must execute a valid business associate agreement with the Entity before disclosing PHI to the Entity. The business associate agreement must contain the elements in 45 CFR §§ 164.314(a) and 164.504(e)

Business Associate Obligations



Business Associate Obligations

- Execute and comply with the terms of the business associate agreement with covered entity.
 - Must contain certain terms required by HIPAA.
- Comply with the Security Rule.
 - Appoint security officer.
 - Perform and document a risk assessment.
 - Implement required safeguards.
 - Execute agreements with subcontractors.
 - Maintain written policies and procedures.
 - Train personnel.
- Comply with minimum necessary standard.
- Report breaches of unsecured PHI to covered entity.

May be difficult for some business associates and subcontractors to comply

Business Associate Obligations

- **Business associates directly liable under HIPAA for:**
 - Use and disclosures in violation of the BAA or the Privacy Rule, including minimum necessary standard.
 - Failing to comply with the Security Rule.
 - Failing to notify covered entity of a reportable breach.
 - Failing to disclose PHI to HHS in response to investigation.
 - Failing to disclose PHI in response to an individual's request for e-PHI.
 - Failing to execute agreements with subcontractors.
 - Failing to address breach by subcontractor.

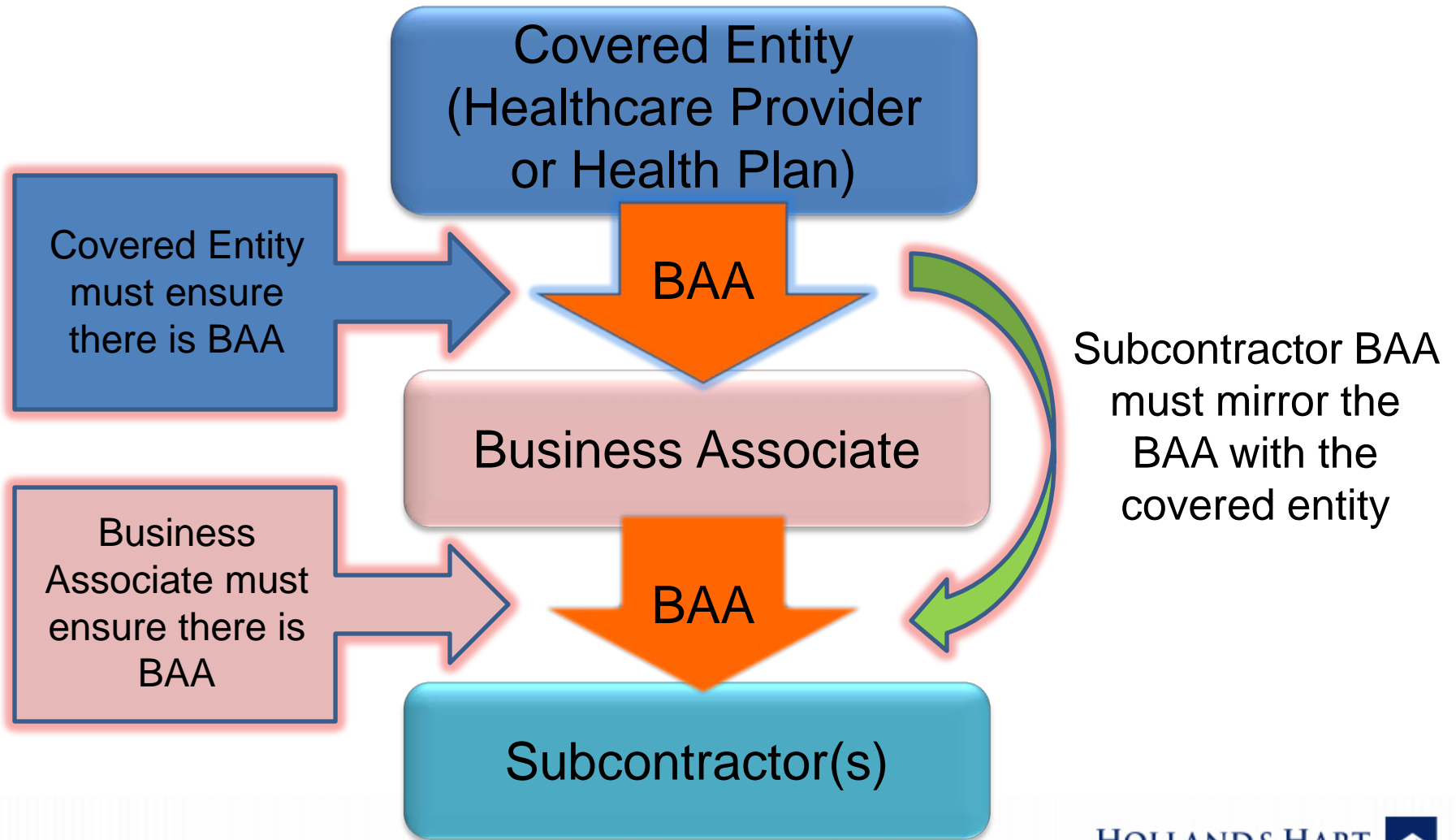
Business Associate Agreements ("BAA")



BAA

- **Covered entity must have BAA before disclosing PHI to business associate or authorizing business associate to create or receive PHI for covered entity.**
 - BAA limits business associate's use of PHI.
- **Business associate must have BAA with subcontractor.**
 - Must match scope of BAA between covered entity and business associate.
- **Must comply with terms of BAA.**
 - Breach of contract with covered entity.
 - HIPAA penalties imposed by OCR.
- **Must comply with HIPAA even if no BAA.**

BAA



BAA: Required Terms

- Establish permitted uses of PHI.
 - Business associate may only use or disclose PHI:
 - As allowed by BAA, or
 - As required by law.
 - May allow business associate to use for its internal management or administration.
 - Business associate may not use or disclose PHI in a manner that would violate the Privacy Rule if done by covered entity.
 - Beware situations where covered entity has limited use or disclosure through, e.g., Notice of Privacy Practices or agreement.

BAA: Required Terms

- **Implement safeguards to protect PHI.**
 - Privacy Rule safeguards are not specified.
- **Comply with HIPAA Security Rule.**
 - Perform and document a risk assessment.
 - Implement administrative, technical and physical safeguards.
 - Execute subcontractor BAAs.
 - Maintain written policies and documentation.
 - Train personnel.

BAA: Required Terms

- Report to covered entity:
 - Breaches of unsecured PHI.
 - Per breach reporting rules.
 - Use or disclosure of PHI not allowed by BAA.
 - HIPAA violations even if not reportable breach.
 - BAA violations even if doesn't violate HIPAA.
 - “Security incidents”, i.e., attempted or successful unauthorized access, use, disclosure, modification, or destruction of info or interference with system operations in an info system.

BAA: Required Terms

- Cooperate in providing individuals with access to PHI in designated record set.
- Cooperate in amending records in designated record set.
- Cooperate in providing accounting of disclosures of PHI in designated record set.
 - Must log improper disclosures and certain disclosures for public safety or government functions, including:
 - Date of disclosure;
 - Name of entity receiving disclosure;
 - Description of info disclosed; and
 - Describe purpose of disclosure.

BAA: Required Terms

- If covered entity delegates its functions to business associate, comply with HIPAA as to those functions.
- Make internal records available to HHS for inspection.
- Execute BAAs with subcontractors.
 - Must parallel BAA with covered entity.
- Authorize termination if business associate violates terms.
- Upon termination of BAA:
 - Return or destroy all PHI if feasible.
 - If not feasible to return or destroy PHI, comply with BAA as to any PHI it retains.

OCR Sample BAA Language

Business Associate Contracts | HHS.gov - Internet Explorer

http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Business Associate Contracts... x

Convert Select File Edit View Favorites Tools Help

Integrated Colorado Courts... Free Hotmail Integrated Colorado Courts... Lexis-Nexis MSN.com Suggested Sites Tarantella Web Slice Gallery Westlaw

HHS.gov

Health Information Privacy

U.S. Department of Health and Human Services

I'm looking for...



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



[HHS Home](#) > [HIPAA](#) > [For Professionals](#) > [Covered Entities](#) > Business Associate Contracts

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Text Resize **A A A**

Print

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS

(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the work entity, who performs functions or activities on behalf of, or provides certain services that involve access by the business associate to protected health information. A business associate also is a subcontractor that creates, receives, maintains, or transmits protected

Beware BAA: Pro-Covered Entity Terms

- Covered entities may want to add these terms:
 - Business associate must report or act within x days.
 - Business associate must implement policies.
 - Business associate must encrypt or implement other safeguards.
 - Business associate must carry data breach insurance.
 - Business associate notifies individuals of breaches and/or reimburses covered entity for costs of the notice.
 - Business associate defends and indemnifies for losses, claims, etc.
 - Business associate is an independent contractor, not agent.
 - Business associate assumes liability for subcontractors.
 - Allow termination of underlying agreement.
 - Must have consent to operate outside the United States.
 - Covered entity has right to inspect and audit.
 - Cooperate in HIPAA investigations or actions.

* *Business associate may want these in subcontracts.*

BAA: Pro-Business Associate Terms

- **Business associates and subs probably want to add these:**
 - Covered entity will not disclose PHI unless necessary.
 - Covered entity will not request action that violates HIPAA.
 - Covered entity has obtained necessary authorizations.
 - Covered entity will not agree to restrictions on PHI that will adversely affect business associate.
 - Covered entity will notify business associate of all such restrictions.
 - Covered entity will reimburse for additional costs.
 - Blanket reporting for security incidents.
 - Specify business associate does not maintain designated record set.
 - Reserve the right to terminate based on restrictions or other change that adversely affects business associate.
 - Subcontractors are independent contractors, not agents.
 - Mutual indemnification.
 - Limitation or cap on damages.

BAA Negotiation

- **Covered entities may require BAA even if you are not a business associate.**
 - If so, explain business associate limits to covered entity.
 - Beware assuming unnecessary liability.
- **Covered entity may insist on BAA terms that are not required or exceed scope of HIPAA.**
 - If so, explain limits.
 - Explain that covered entity generally is not liable for acts of business associate.
- **As a practical matter, you may have to agree to BAA terms if you want to do business with the covered entity.**

BAA: Summary

- **Do not assume BAA liability unless you must.**
- **Review terms of BAA carefully.**
 - Beware terms that are not required by HIPAA.
 - Beware terms that increase liability.
 - Negotiate more favorable terms if you can.
- **Ensure you comply with BAA terms.**
 - Ensure your workforce understands requirements.
 - You likely must report disclosures in violation of BAA.
 - Disclosures in violation of BAA are HIPAA violations.

HIPAA Security Rule

(45 CFR 164.300 et seq.)



Security Rule

- **Designed to protect electronic PHI (“e-PHI”)**
 - Confidentiality
 - Integrity
 - Availability
- **General requirements**
 - Conduct risk analysis of system vulnerabilities.
 - Implement specific administrative, technical and physical safeguards.
 - Execute business associate agreements.
 - Maintain written policies.
 - Train personnel.

Security Rule: The Good News

- **Most of this stuff is not rocket science.**
- **Involves common sense precautions to protect your business or organization.**
 - **Protect information necessary to carry on business.**
 - **Protect systems used in business.**
 - **Protect individuals' information.**
- **You are probably already doing most of this stuff.**
- **If you aren't doing it, you should be doing it for your own protection...**

Remember...



DATA BREACHES

DATA RECORDS LOST OR STOLEN IN 2014

1,023,108,267

2,803,036
records lost or stolen
every day



116,793
records
every hour



1,947
records
every minute



32
records
every second



ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

RECORDS BREACHED IN FIRST HALF OF 2015

245,919,393

NUMBER OF BREACH INCIDENTS

888

TOP 10 BREACHES
PERCENTAGE OF TOTAL RECORDS

THE FOLLOWING FREQUENCY

EVERY
DAY
1,358,671

EVERY

HOLLAND & HART



Security Rule: Risk Analysis

- Must “[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.” (45 CFR 164.308(a))
- No particular analysis required.
- Analysis may vary depending on size and resources.
- May conduct analysis internally.
- Analysis should be ongoing.

HHS Guidance re Risk Analysis

Final Guidance on Risk Analysis | HHS.gov - Internet Explorer

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

Final Guidance on Risk Analy... x

Convert Select File Edit View Favorites Tools Help

Integrated Colorado Courts... Free Hotmail Integrated Colorado Courts... Lexis-Nexis MSN.com Suggested Sites Tarantella Web Slice Gallery Westlaw

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services

I'm looking for...

HHS A



HIPAA for
Individuals



Filing a
Complaint



HIPAA for
Professionals



Newsroom

[HHS Home](#) > [HIPAA](#) > [For Professionals](#) > [Security](#) > [Guidance](#) > Final Guidance on Risk Analysis

HIPAA for Professionals

Privacy



Security



[Summary of the Security Rule](#)

[Guidance](#)

[Combined Text of All Rules](#)

Breach Notification



Text Resize **A A A**

Print

Share

Final Guidance on Risk Analysis

The Office for Civil Rights (OCR) is responsible for issuing periodic guidance on the provisions of the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) This series of guidance documents will assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The materials will be updated annually, as appropriate.

[View the Final Guidance on Risk Analysis.](#)

HHS Risk Assessment Tool



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 AssessmentTool

Security Risk AssessmentVideos

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, available at no cost, can be downloaded from Apple's [App Store](#).

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)

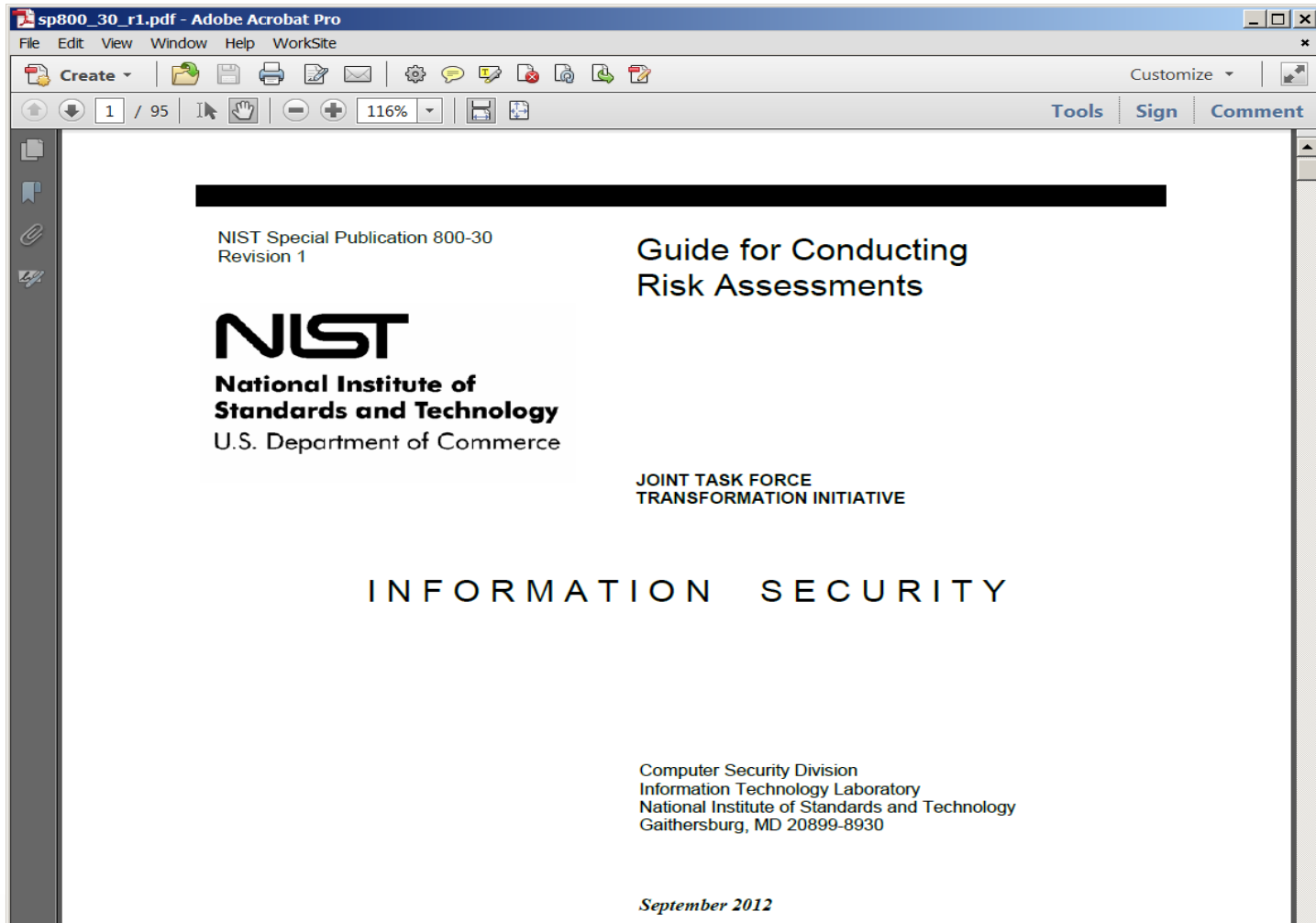


[Download Tool](#)

SRA Tool (iPad version)

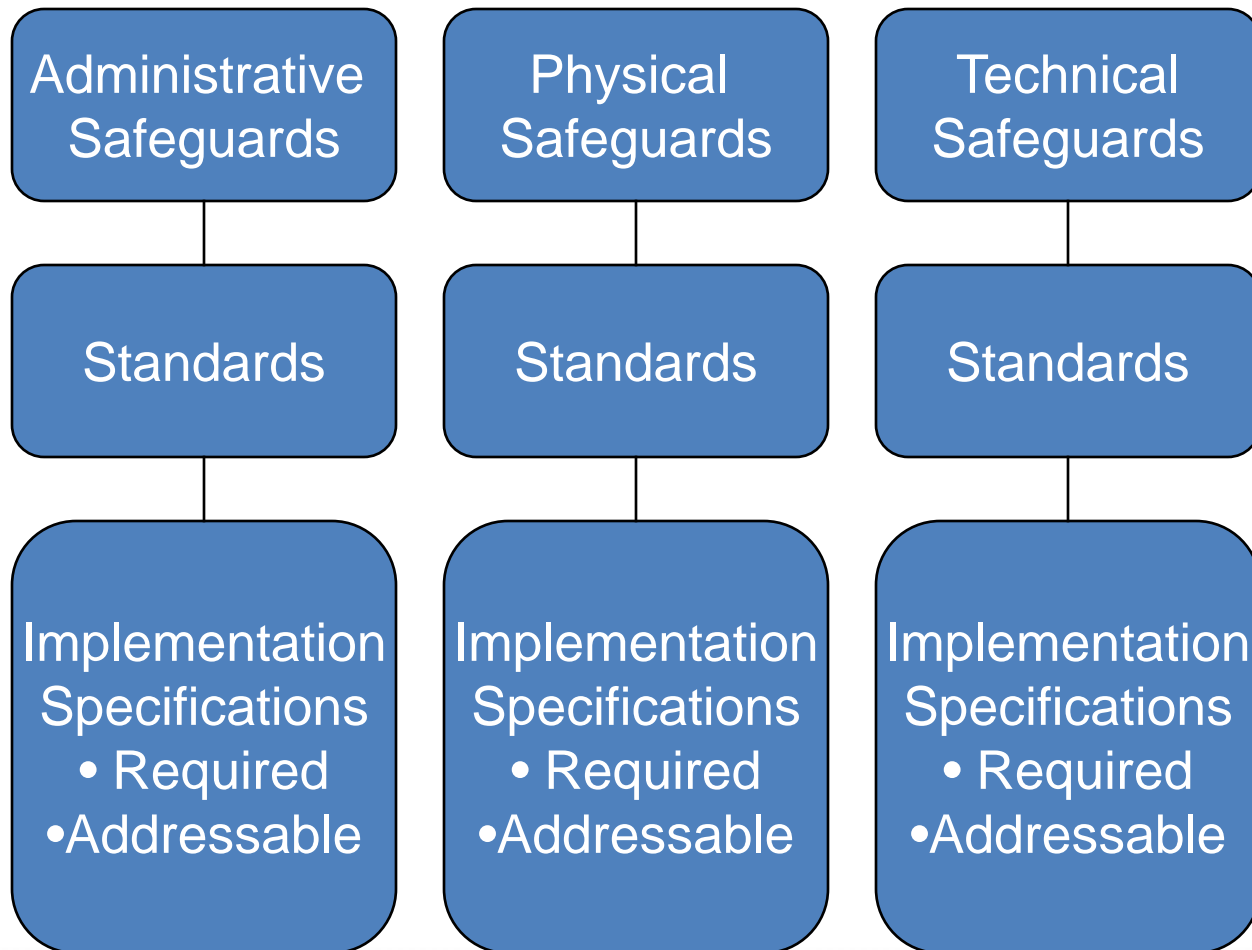
NIST Special Publication 800-30

Revision 1 (Sept. 2012)



Security Rule: Safeguards

(45 CFR 164.308-.312)



Security Rule: Safeguards

- “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 (164.308)

- **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.**

Security Rule: Physical Safeguards (164.310)

- **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.**

Security Rule: Technical Safeguards (164.312)

- **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.**

OCR Security Rule Guidance

Security Rule Guidance Material | HHS.gov - Internet Explorer

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

Security Rule Guidance Mate... x

Convert Select File Edit View Favorites Tools Help

Integrated Colorado Courts... Free Hotmail Integrated Colorado Courts... Lexis-Nexis MSN.com Suggested Sites Tarantella Web Slice Gallery Westlaw

HHS.gov

Health Information Privacy

U.S. Department of Health & Human Services

HIPAA for Individuals

Filing a Complaint

HIPAA for Professionals

Newsroom

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 Simplification Rules

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-P

[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](#)

[Security Standards: Implementation for the Small Provider](#)

OCR Security Series

Security Rule Guidance Material | HHS.gov - Internet Explorer

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

Security Rule Guidance Mate...

Convert Select File

Integrated Colorado Cour

security101.pdf - Adobe Acrobat Pro

File Edit View Window Help WorkSite

Create Save Print Comment Mail Settings Help

Customize

1 / 11 116%

Tools Sign Comments



Security Topics

★ 1.
Security 101 for Covered Entities

2.
Security Standards - Administrative Safeguards

3.
Security Standards - Physical Safeguards

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 the Protection of Electronic Protected Health Information", found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The topics are:

Compliance Deadlines

No later than April 20, 2005 for all covered entities except small health plans which have until no later than April 20, 2006.

HealthIT.gov

Mobile Health Security: Mobile Health Device Privacy and Security | Providers & Professionals | - Windows Internet Explorer pro

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

File Edit View Favorites Tools Help

Convert Select

Favorites HH Secure HIPAA (160) AHILA Lists AKS (2) AKS CMS home CMS Stark eCFR EMTALA guidelines Gmail HIPAA Hotmail Idaho Statutes IDAPA DHW IDSOS Search

Mobile Health Security: Mobile Health Device Pri...

Blog | Federal Advisory Committees (FACAs) | Contact | Get Email Updates | RSS | Twitter | YouTube | SoundCloud | LinkedIn | Google+



in Partnership with the
National Learning Consortium

Newsroom | FAQs | Multimedia

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

Worried About Using a Mobile Health Device for ...

MOBILE DEVICE RISKS

- 1) Lost mobile device
- 2) Stolen mobile device
- 3) Downloaded virus

Done

Internet | Protected Mode: Off

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.**

Security Rule: Summary

- Document your good faith risk analysis.
- Work with IT to implement the safeguards in 45 CFR 164.308-.312.
 - If addressable, document evaluation.
- Develop policies concerning the safeguards.
- Execute business associate agreements.
- Train personnel.
- Respond promptly to any violation.
- Document your actions.

Privacy Rule

(45 CFR 164.500 et seq.)



Privacy Rule:

Use and Disclosure of PHI

- **Business associate may only access, use or disclose PHI as permitted or required by the BAA or applicable law.**
 - **Make sure BAA authorizes your uses or disclosures.**
 - **Cannot use the PHI internally unless allowed by your BAA.**
- **Business associate cannot disclose PHI to subcontractor unless they have a BAA.**
 - **Make sure you have a BAA with subcontractors.**
 - **BAA must track the limits in the BAA with the covered entity.**

Privacy Rule:

Use and Disclosure of PHI

- **Business associate may not access, use or disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity.**
 - **Business associate must comply with:**
 - **HIPAA Privacy Rule limits on use or disclosure**
 - **Additional restrictions imposed by covered entity.**
 - **Business associate should confirm whether covered entity has agreed to additional restrictions through notice of privacy practices or other agreements.**

Privacy Rule:

Use and Disclosure of PHI

- Covered entity and business associate may not access, use or disclose PHI unless—
 - For purposes of the covered entity’s treatment, payment, or healthcare operations;
 - As required by other laws;
 - For certain safety or government purposes as listed in 45 CFR 164.512; or
 - Have valid written authorization from individual.
- Business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish intended purpose for the use, disclosure or request.
 - “Minimally necessary standard”

Privacy Rule: Use and Disclosure of PHI

Privacy Rule net effect:

- *Don't access, use or disclose PHI unless:*
 - *Within scope of your services agreement or BAA,*
or
 - *Directed to disclose it by covered entity.*
- *Do not request, access, use or disclose more than is minimally necessary for requested purpose.*

Privacy Rule:

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 healthcare.
 - See OCR Guidance at www.hhs.gov/hipaa/for-professionals/privacy/guidance

Privacy Rule: Tracking Disclosures

- BAA requires business associates to assist covered entities in accounting for disclosures per 45 CFR 164.528.
- BAA must track:
 - Disclosures in violation of HIPAA.
 - Disclosures required by law, to avoid serious harm, or to certain government agencies per 45 CFR 164.512.
- BAA should log:
 - Date of disclosure.
 - Name and address of entity to whom disclosure made.
 - Describe PHI that was disclosed.
 - Describe purpose of disclosure.
- Report improper disclosures to covered entity.

HIPAA Breach Notification

(45 CFR 164.400 et seq.)



Breach Notification

- If there is a breach of unsecured PHI,
 - Business associate must notify covered entity.
 - Covered entity must notify:
 - Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed.
 - HHS.
 - Media, if more than 500 persons affected.
- Reports may likely result in:
 - Patient complaints
 - OCR investigations
 - Costs and potential penalties

“Unsecured” 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 National Institute of Standards and Technology (NIST).
- **Destruction of PHI.**
 - Paper, film, or hard copy media is shredded or destroyed such that info cannot be read or reconstructed.
 - Electronic media is cleared, purged or destroyed consistent with NIST standards.
- **Guidance updated annually.**

(74 FR 42742 or www.hhs.gov/ocr/privacy)

Breach

- 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.

Breach

- **“Breach” does not include 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.**

To determine if breach occurred

- 1) Was there access, use or disclosure of PHI?
- 2) Did it violate the Privacy Rule?
- 3) Is there a low probability that the info has been “compromised”?
 - Risk assessment
- 4) 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.

** Document foregoing.*

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 (or time stated in BAA).**
 - **“Discovery” = time that anyone (except violator) knew or should have known of the breach.**
 - **Notice shall include to extent possible:**
 - **Identification of individuals affected.**
 - **Description of what happened, including date of breach and discovery.**
 - **Description of type of PHI affected.**
 - **What is being done to mitigate.**

Notice by Business Associates

- In addition to reportable “breaches” of PHI, business associate must also report to covered entity:
 - Uses or disclosures in violation of HIPAA.
 - Uses or disclosures in violation of the BAA.
 - “Security incidents”, i.e., attempted or successful unauthorized access, use, disclosure, modification, or destruction of info or interference with system operations in an info system.
- BAA may impose additional requirements on business associate re breaches or reports.

Costs of Notice

- If have breach of unsecured PHI involving 500+ persons—
 - Time and cost to investigate facts.
 - Time and cost to prepare, send, and pay for letters to 500 patients, personal representatives, or next of kin.
 - Time and cost to respond to inquiries from individuals, e.g., even if 20% respond, that is 100 patients.
 - Cost of toll-free number for 90 days.
 - Cost of media notices and website updates.
 - Notice may lead to additional actions by—
 - Angry clients or individuals.
 - HHS enforcement
 - Media inquiries
 - Potential loss of business due to adverse publicity.
- *Better to comply!*

If you think you have a breach

- Act immediately to mitigate or correct the breach.
 - Retrieve the info.
 - Confirm that the info has not been improperly accessed, used or disclosed, or if it has, obtain assurance that it will not be further disclosed.
- Notify supervisor immediately.
- Notify the covered entity if required.
- Correct any process that resulted in improper disclosures.
- Remember: prompt action may allow parties to—
 - Satisfy duty to mitigate.
 - Avoid disclosure and breach reporting obligation.
 - Defend against HIPAA penalties.

Liability for Acts of Business Associates or Subs

Independent Contractor



Or Employee

Liability for Acts of Business Associate or Subs

- **Covered entity or business associate violates HIPAA if:**
 - **Knew of a pattern of activity or practice of the business associate/subcontractor that constituted a material breach or violation of the business associate’s/subcontractor’s obligation under the contract or other arrangement;**
 - **Failed to take reasonable steps to cure the breach or end the violation, as applicable; or**
 - **Failed to terminate the contract or arrangement, if feasible.**

(45 CFR 164.504(e)(1))

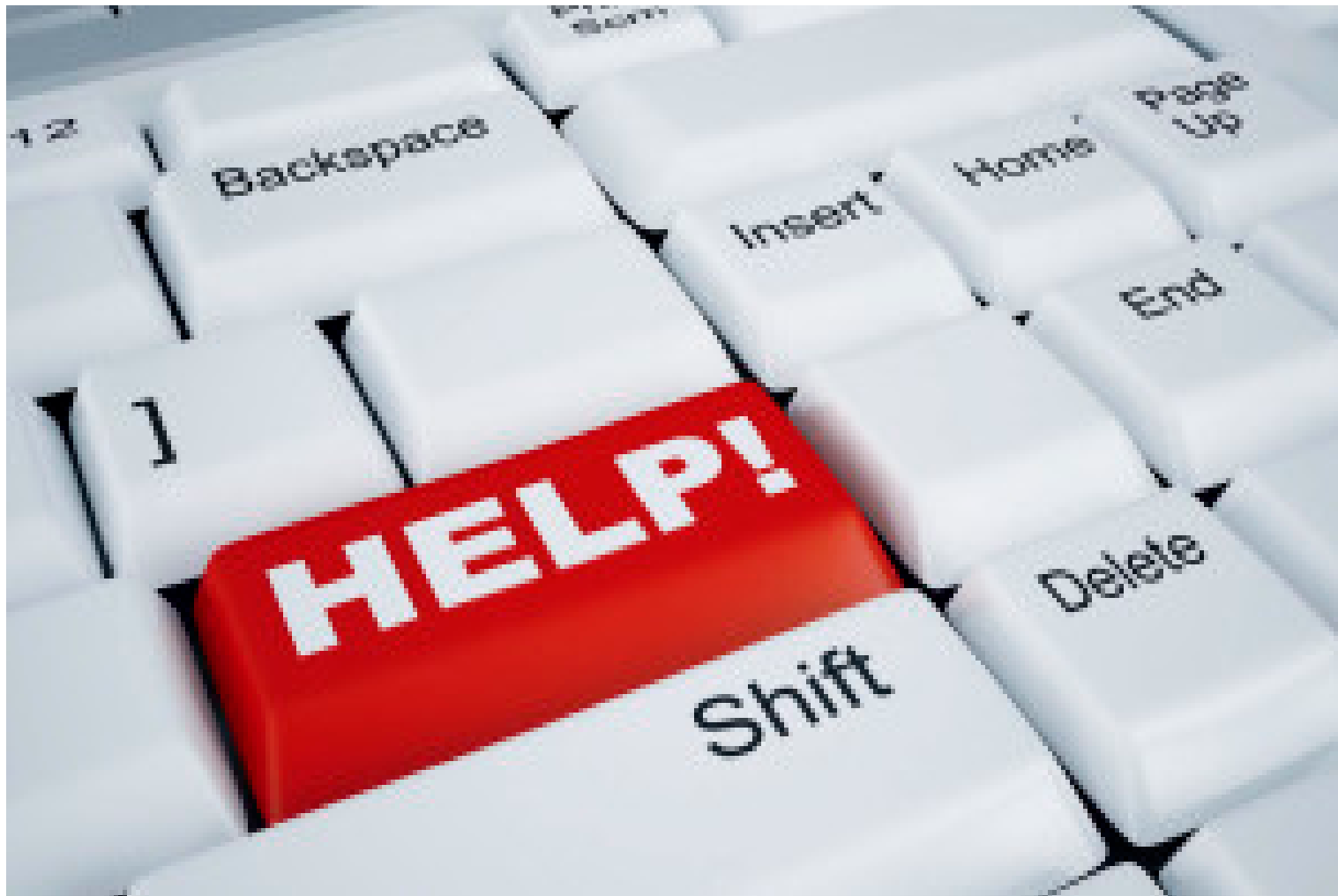
Liability for Acts of Business Associate of Subs

- Covered entity or business associate is liable, in accordance with the Federal common law of agency, for the acts or omissions of a business associate/subcontractor acting with the scope of the agency.
(45 CFR 160.402(c)).

- Test: right or authority of a covered entity to control the business associate's conduct.
- Factors:
 - Contract terms.
 - Right to give interim directions or control details.
 - Relative size or power of the entities.

- *Maintain independent contractor status!*
(78 FR 5581-82)

Additional Resources



www.hhs.gov/hipaa

Health Information Privacy | HHS.gov - Internet Explorer

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

Health Information Privacy | HH... Health Information Privacy |...

Convert Select File Edit View Favorites Tools Help

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](#) > Health Information Privacy

Text Resize A A A

Print

Share



Health Information Privacy

I would like info on. . .

> [Your Rights under HIPAA](#)

> [Covered Entities and Business Associates](#)

> [HIPAA Enforcement Highlights](#)

> [Frequently Asked Questions](#)



[HIPAA Access Guidance and FAQs](#)

New guidance and FAQs clarify HIPAA's Right to Access requirements.

HIPAA for Individuals

We offer information about your rights under HIPAA and answers to frequently asked questions about the HIPAA Rules.

Filing a HIPAA Complaint

You may file a complaint with OCR if you feel your rights under the HIPAA Rules were violated.

HIPAA for Professionals

Find information about the HIPAA Rules, guidance on compliance, OCR's enforcement activities, frequently asked questions, and more.

HealthIT.gov

Providers & Professionals

healthit.gov/providers-professionals

Blog Federal Advisory Committees (FACAs) Contact Get Email Updates



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

What's in IT for you?

Learn about incentives for certification and find out how you can get paid for going paperless.

[Learn More >](#)



1 2 3 4 ||

Print | Share

Take the First Step Toward EHR Implementation

Whether you're just starting to think about adopting an electronic health record (EHR) system or are ready to make the change from paper records to EHRs, find out how to get started.

[Take the First Step >](#)

Achieve Meaningful Use

Already have an EHR System? Learn about the meaningful use objectives that eligible professionals and hospitals must achieve to qualify for Centers for Medicare & Medicaid Services (CMS) Incentive Programs.

[Achieve Meaningful Use >](#)

Get Local Technical Help

The EHR adoption process can be overwhelming. But you don't have to do it alone. The nationwide network of Regional Extension Centers (RECs) offers local, low-cost, on-the-ground support.

[Get Local Technical Help >](#)

Holland & Hart Website

people

practices

firm

locations

news & resources

careers

diversity & inclusion

community

Contact
Disclaimer
Site Map

Healthcare

Overview

Holland & Hart provides a comprehensive health law practice to assist clients in navigating the dynamic healthcare industry. In recent years, healthcare has experienced dramatic change, extraordinary competition, and increasingly complex regulation. Our experienced attorneys and staff skillfully respond to these challenges. By remaining on the forefront of healthcare law, we are able to provide coordinated services to meet the business, transactional, litigation, and regulatory needs of our clients.

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



Contact



Kim C. Stanger

View Profess

- Related P
- Business/
- Litigation
- Complian
- Audits, an

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

[+ Read More](#)

[+ Expand All](#)

- Publications

HHS Issues New Rule Prohibiting Discrimination Based on Sex and Requiring Interpreters

Holland & Hart News Update

Author(s): **Patricia Dean**

US District Court Decision Provides Cautionary Tale on False Claim Act Requirement to Return Identified Overpayments from Medicare or Medicaid

Holland & Hart News Update

Author(s): **Patricia Dean**

Recruiting Physicians: Beware Stark, Anti-Kickback Statutes, and IRS Rules

HIPAA Resources



Questions?

Teresa D. Locke

Holland & Hart LLP

tlocke@hollandhart.com

(303) 295-8480

