HIPAA Business Associates

Kim C. Stanger
(2/17)

HOLLAND&HART

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

HOLLAND&HART

Holland & Hart Webinar Series

Our 2017 HIPAA Compliance Webinars:

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

Webinars and materials are available at http://www.hhhealthlawblog.com/webinar-recordings-and-presentations.

HOLLAND&HART

Overview

- Why should you care about business associates?
- 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

- Written materials
  - .ppt slides
  - OCR, *Terms for Business Associate Agreement.*
  - OCR, *Guidance on HIPAA & Cloud Computing.*
  - Stanger, *Business Associate Decision Tree.*
  - Stanger, *Complying with HIPAA: A Checklist for Business Associates*
  - Stanger, *Checklist for Business Associate Agreements*.
  - Stanger, *Avoiding Business Associate Agreements*.
- Written materials are available per the webinar instructions or contact me at kcstanger@hollandhart.com.
- Submit questions per Web-Ex "chat" function or contact me at kcstanger@hollandhart.com.

HOLLAND&HART

Why you should care about HIPAA and business associates

HIPAA Liability

- HIPAA penalties apply to:
  - Covered entities
    - Healthcare providers who engage in certain electronic transactions.
    - Health plans, including employee group plans:
      - with 50 or more participants, or
      - that are administered by a third party.
    - Healthcare clearinghouses.
  - Business associates, including subcontractors of business associates.

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	• $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

Civil Penalties

(45 CFR 160.404)

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

HIPAA Fines/Settlements Over Last Year

Conduct	Penalty
Loss or theft of unencrypted devices with info of 7,000+ patients	$3,200,000
Theft of unencrypted USB with info of 2,209 individuals	$2,200,000
Patient info accessible through internet searches	$2,140,500
BA lost unencrypted backup tapes of 14,000 persons; CE liable for failing to review and update BAA to include privacy and security rule requirements.	$400,000
Widespread breaches involving 4,000,000 persons; among other things, CE failed to obtain BAAs.	$5,500,000
Theft of unencrypted laptop exposing info of 10,000 patients	$2,750,000
BA lost x-rays of 17,300 patients; CE liable for failing to execute a BAA	$750,000
Hospital laptop containing 13,000 patients' info stolen from car	$3,900,000
BA's laptop containing 9,497 patients' info stolen; CE liable for failing to execute a BAA	$1,550,000
Theft of BA's unsecured iPhone containing info of 412 persons.	$650,000

Press Release **Thursday, January 19, 2012**

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

Lessons from recent settlements

- Covered entities:
  - Ensure you have BAAs in place.
  - Ensure your BAAs comply with 2013 omnibus rule requirements.
- Business associates:
  - Ensure you comply with—
    - HIPAA security rules.
    - BAA terms.

Who are Business Associates?

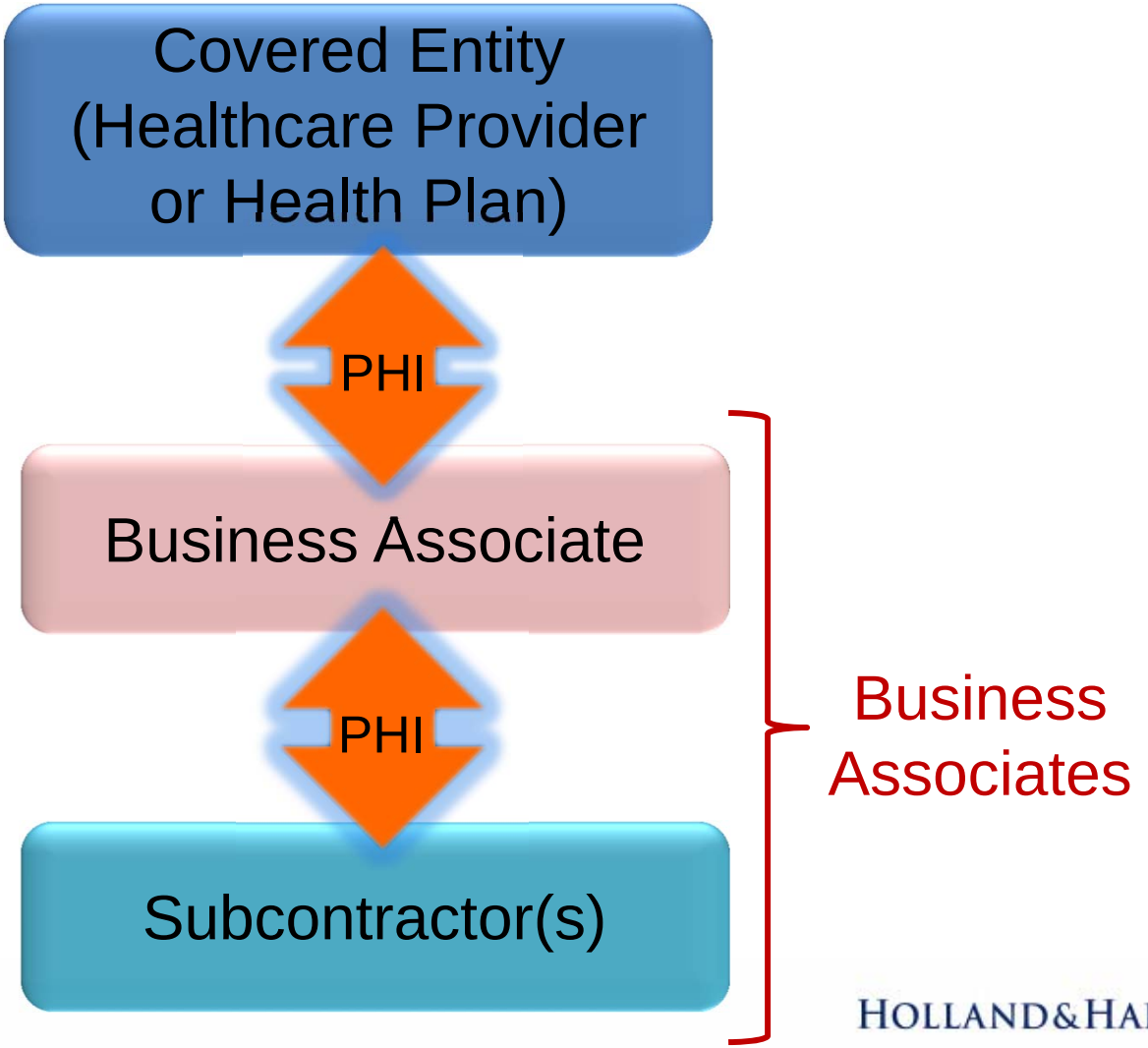
HOLLAND&HART

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 or data is encrypted.
  - Patient safety organizations.
- Covered entities acting as business associates.
- Subcontractors of business associates.

Business Associates



HOLLAND&HART

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.
- 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 <u>not</u> 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 <u>not</u> 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 <u>not</u> 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?

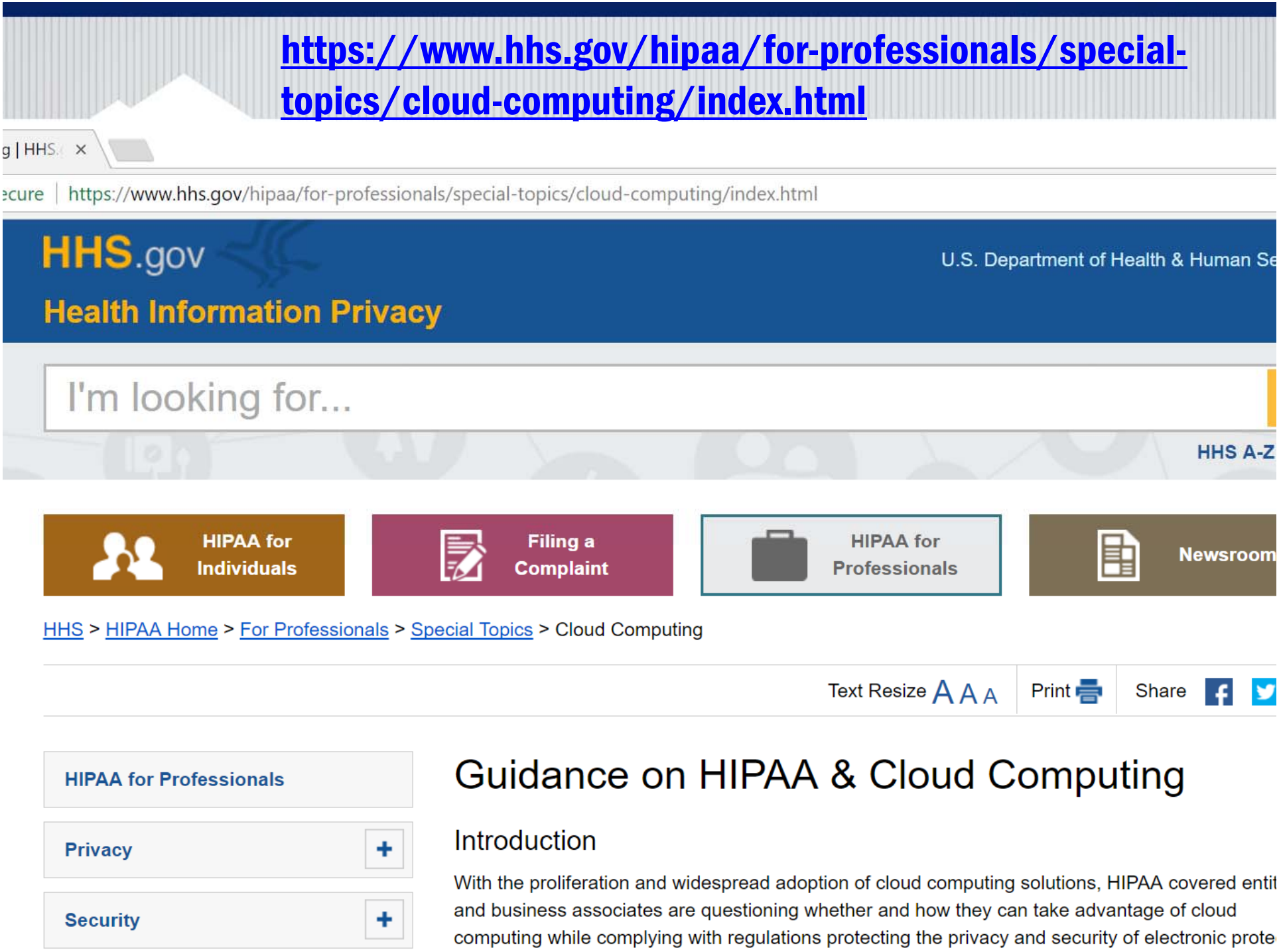
No → The Entity is <u>not</u> a business associate

Yes ↓

The Entity <u>is</u> 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)

HOLLAND&HART

https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html



Cloud Services Providers

- CSPs are BAs if they store PHI even though:
  - They do not access data.
  - Data is encrypted and CSP does not have access key.
    - Must still ensure the availability and integrity as well as confidentiality of the e-PHI.
- Must have BAA with CSP.
- CSP not liable if it did not know CE was using CSP to create, receive, maintain or transmit PHI.
  - Upon learning of such acts, CSP must correct situation within 30 days.

Business Associate Obligations

HOLLAND&HART

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.

May be difficult for some business associates and subcontractors to comply

- Comply with minimum necessary standard.
- Report breaches of unsecured PHI to covered entity.

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.

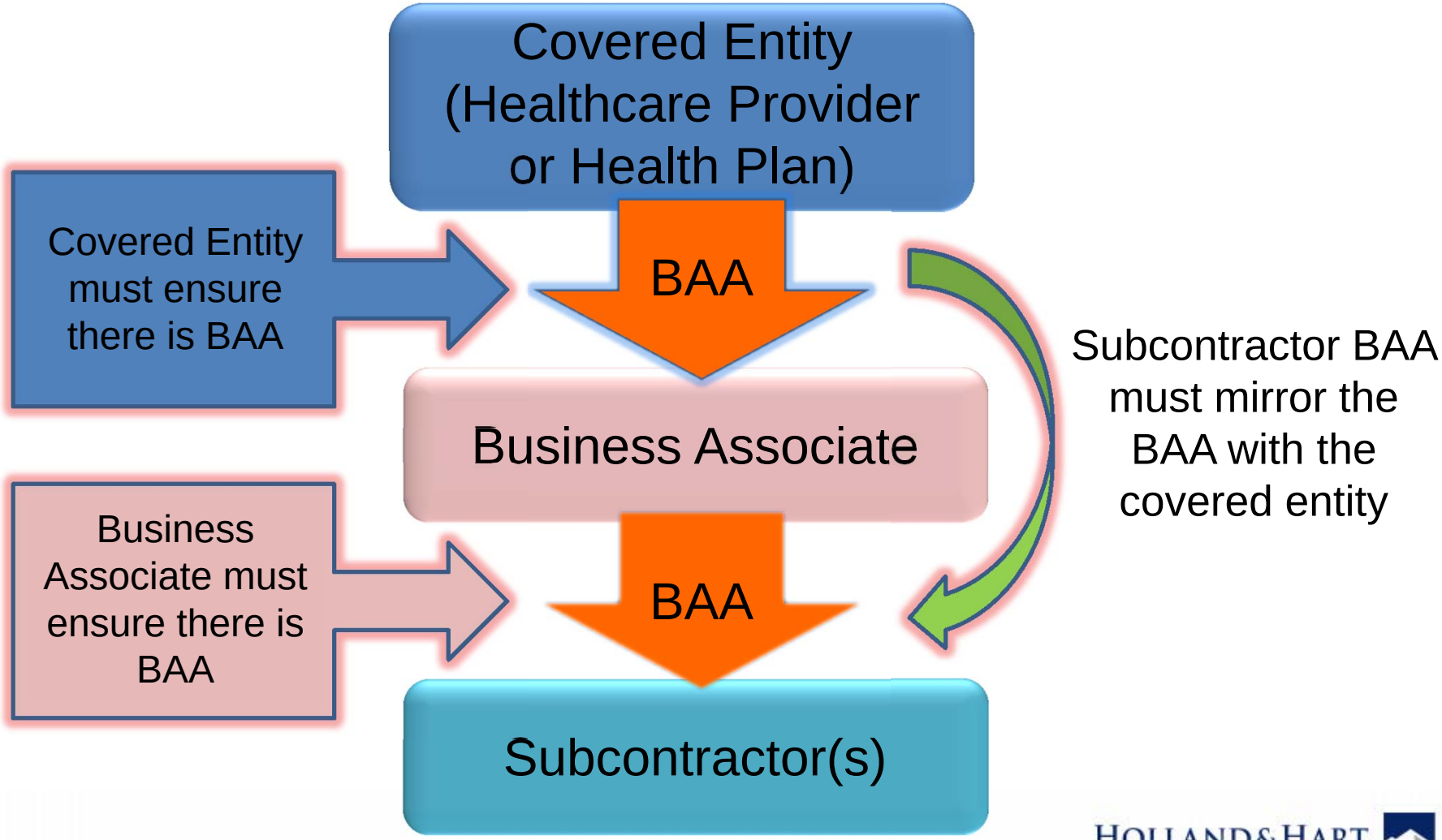
Business Associate Agreements ("BAA")

HOLLAND&HART

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



HOLLAND&HART

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.

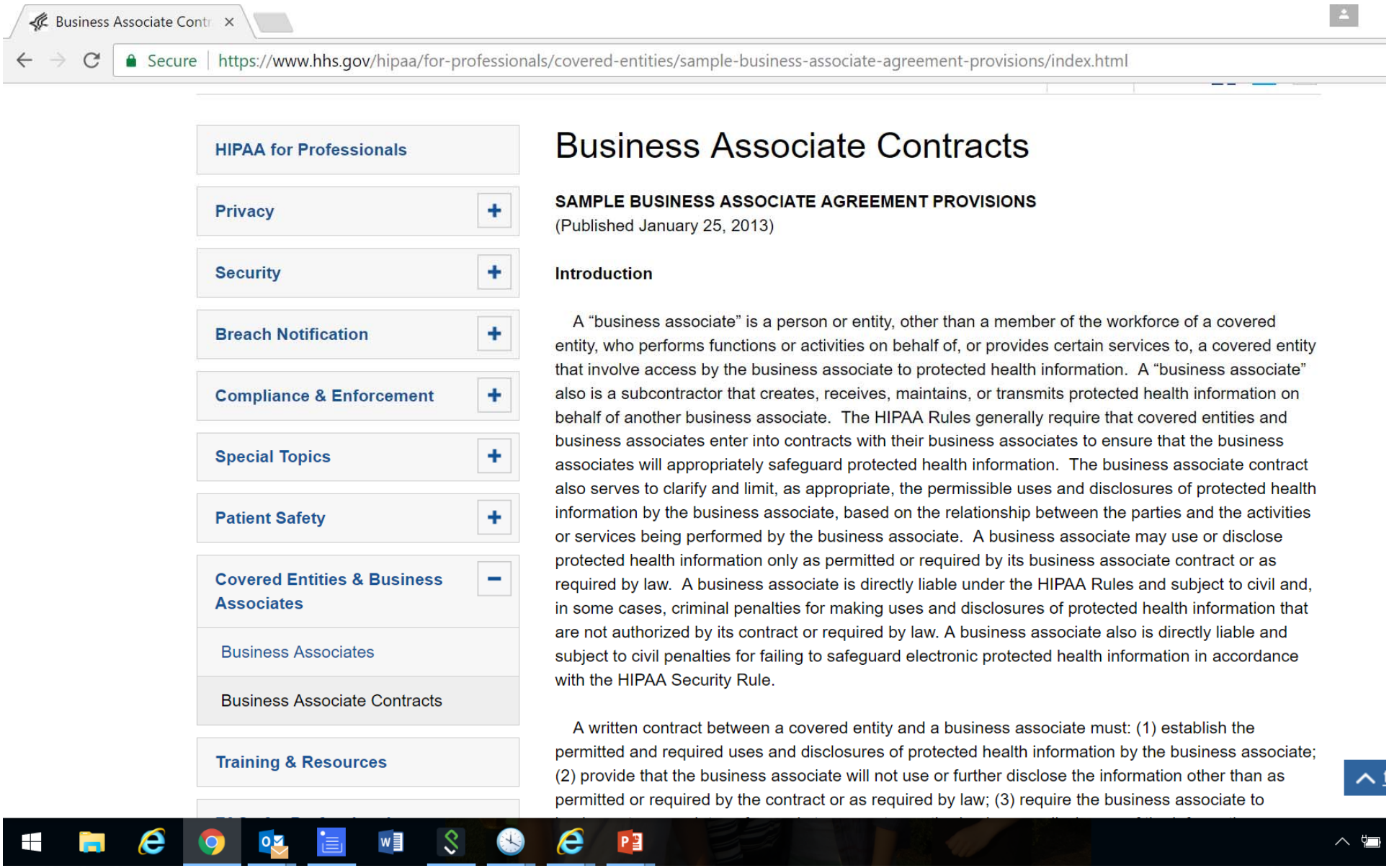
BAA: Required Terms

- 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.

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



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.*

HOLLAND&HART

BAA: Pro-BA 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

It comes down to bargaining power…

HOLLAND&HART

BAA Negotiation

- Covered entities often require BAA even if contractor is not a BA as defined by HIPAA.
  - Covered entity may not understand definition of BA.
  - Covered entity may want to play it safe.
  - BA may want to explain or make BAA conditional on BA status.
  - BA may want to propose confidentiality agreement instead.
- Covered entities may insist on BAA terms that are not required or exceed scope of HIPAA.
  - Matter of contract negotiation.
- As a practical matter, BA may have to agree to BAA terms if it wants to do business with the covered entity.

BAA: Summary

- CEs: when in doubt, demand BAA.
- BAs: 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.
- Remember: if you are a BA, you must comply with HIPAA requirements whether or not you have a BAA.
- 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.)

- If business associate creates, receives, maintains or transmits electronic PHI….

HOLLAND&HART

Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potentia violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule afte the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

"Business associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities," said U.S Department of Health and Human Services Office for Civil Rights (OCR) Director Jocelyn Samuels. "This includes an enterprise-wide risk analysis and corresponding risk management plan, which are th cornerstones of the HIPAA Security Rule." OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issuec employee iPhone. The iPhone was unencrypted and was not password protected. The information or the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile

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.

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

ssment ×

cure | 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

Security Risk Assessment Tool

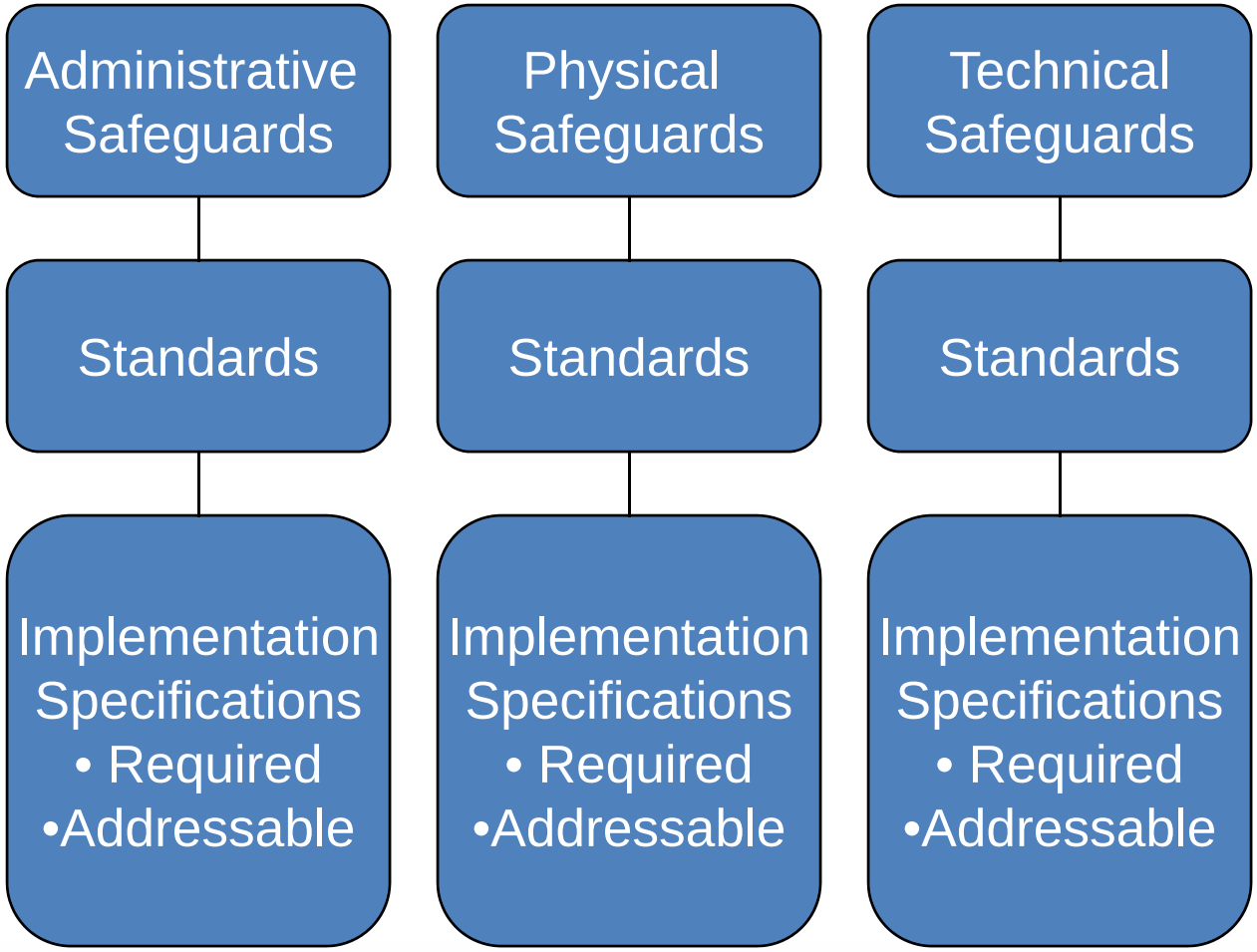
What is the Security Risk Assessment Tool (SRA Tool)?

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

SRA Tutorial Video

Security Rule: Safeguards

(45 CFR 164.308-.312)



HOLLAND&HART

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)

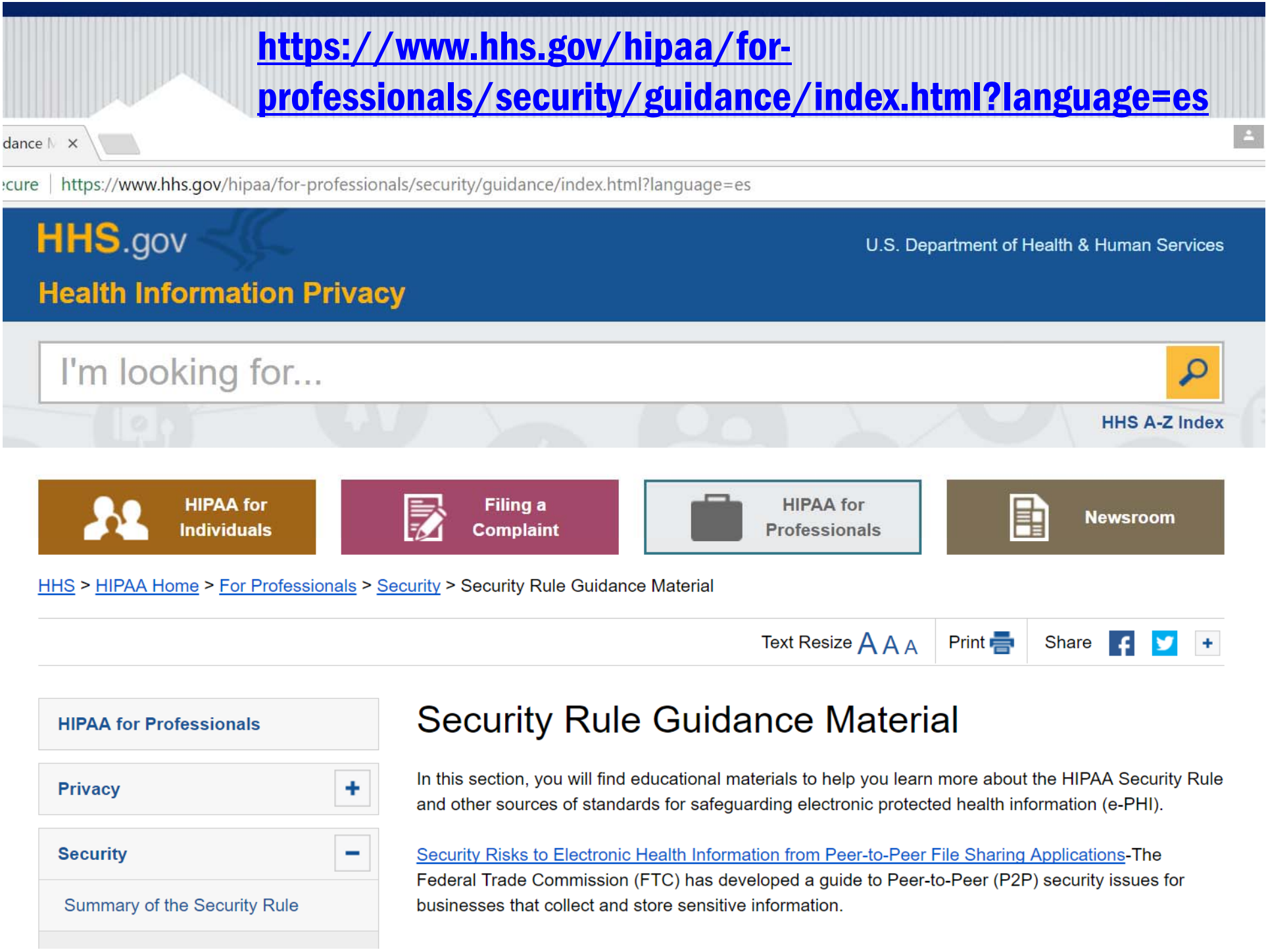
- Limit access to physical facilities and devices containing e-PHI.
- Document repairs and modifications to facilities.
- Secure workstations.
- Implement policies concerning proper use of workstations.
- Implement policies concerning the flow of e-PHI into and out of the facility.
- Implement policies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

HOLLAND&HART

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es



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.)

HOLLAND&HART

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 any uses or disclosures.
  - BA may not use the PHI internally unless allowed by BAA.
- Business associate may not disclose PHI to subcontractor unless they have a BAA.
  - BA: 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"

HOLLAND&HART

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/ocr/hipaa/privacy

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.

HOLLAND&HART

Privacy Rule: De-Identifying Info

- BAA may authorize business associate to "de-identify" PHI if covered entity chooses.
  - Include in BAA.
  - Once info is "de-identified", HIPAA no longer applies to it and business associate may use it.
- Business associate may not de-identify or use de-identified info unless authorized by covered entity.

Terminating Access

- BA may not impermissibly block or terminate covered entity's access to PHI.
  - Privacy Rule prohibits BA's improper "use" through blocking or terminating access to the customer, e.g., "Kill switch" in software following payment dispute.
  - Security Rule requires BA to ensure the confidentiality, integrity and availability of e-PHI.
- Upon termination, BA must return PHI as provided in BAA.

(See FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html?language=es)

HOLLAND&HART

Terminating Access

- Covered entity may not agree with BA to terms that would prevent the covered entity from being able to access or obtain its PHI.

(See FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html?language=es)

HIPAA Breach Notification

(45 CFR 164.400 et seq.)

HOLLAND&HART

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

HOLLAND&HART

"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.

HOLLAND&HART

Notice by Business Associate

- Business associate must notify covered entity of breach of unsecured PHI.
  - Without unreasonable delay but no more than 60 days from discovery (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.

Reporting "Security Incidents"

- "The Security Rule … is flexible and does not prescribe the level of detail, frequency, or format of reports of security incidents, which may be worked out between the parties to the business associate agreement (BAA). For example, the BAA may prescribe differing levels of detail, frequency, and formatting of reports based on the nature of the security incidents – e.g., based on the level of threat or exploitation of vulnerabilities, and the risk to the ePHI they pose. The BAA could also specify appropriate responses to certain incidents and whether identifying patterns of attempted security incidents is reasonable and appropriate."

(https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html).

Reporting "Security Incidents"

- A BA "may decide that certain types of attempted or successful security incidents or patterns of attempted or successful incidents, such as a "ping" (a request-response utility used to determine whether a specific Internet Protocol (IP) address, or host, exists or is accessible) on the [BA's] communications network initiated from an external source, could be reported to the [CE] in a monthly report that only includes an aggregate number of pings that month. Based on its analysis, the [BA] may also determine that other types of incidents, such as suspicious patterns of "pings" on the [CE's] communications network initiated from an external source, or a specific malicious security incident, would require a detailed report to the [CE] as soon as the [BA] becomes aware of them."

(https://www.hhs.gov/hipaa/for-professionals/faq/2016/under-the-security-rule-must-plan-sponsors-report-security-incidents-to-the-group-plan/)

Liability for Acts of Business Associates or Subs

HOLLAND&HART

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))

- Maybe if failed to execute BAA.
  - See recent settlements.

HOLLAND&HART

Liability for Acts of Business Associate of Subs

- CE or BA is liable, in accordance with the Federal common law of agency, for the acts or omissions of a BA/sub-BA acting with the scope of the agency.

(45 CFR 160.402(c)).

- Test: right or authority of a CE covered entity to control the BA's conduct.
  - 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)

No Duty to Monitor BA

- "[HIPAA] does not require a covered entity to actively monitor the actions of its business associates .... Rather, the Rule only requires that, where a covered entity knows of a pattern of activity or practice that constitutes a material breach or violation of the business associate's obligations under the contract, the covered entity take steps to cure the breach or end the violation. See § 164.504(e)(1)."

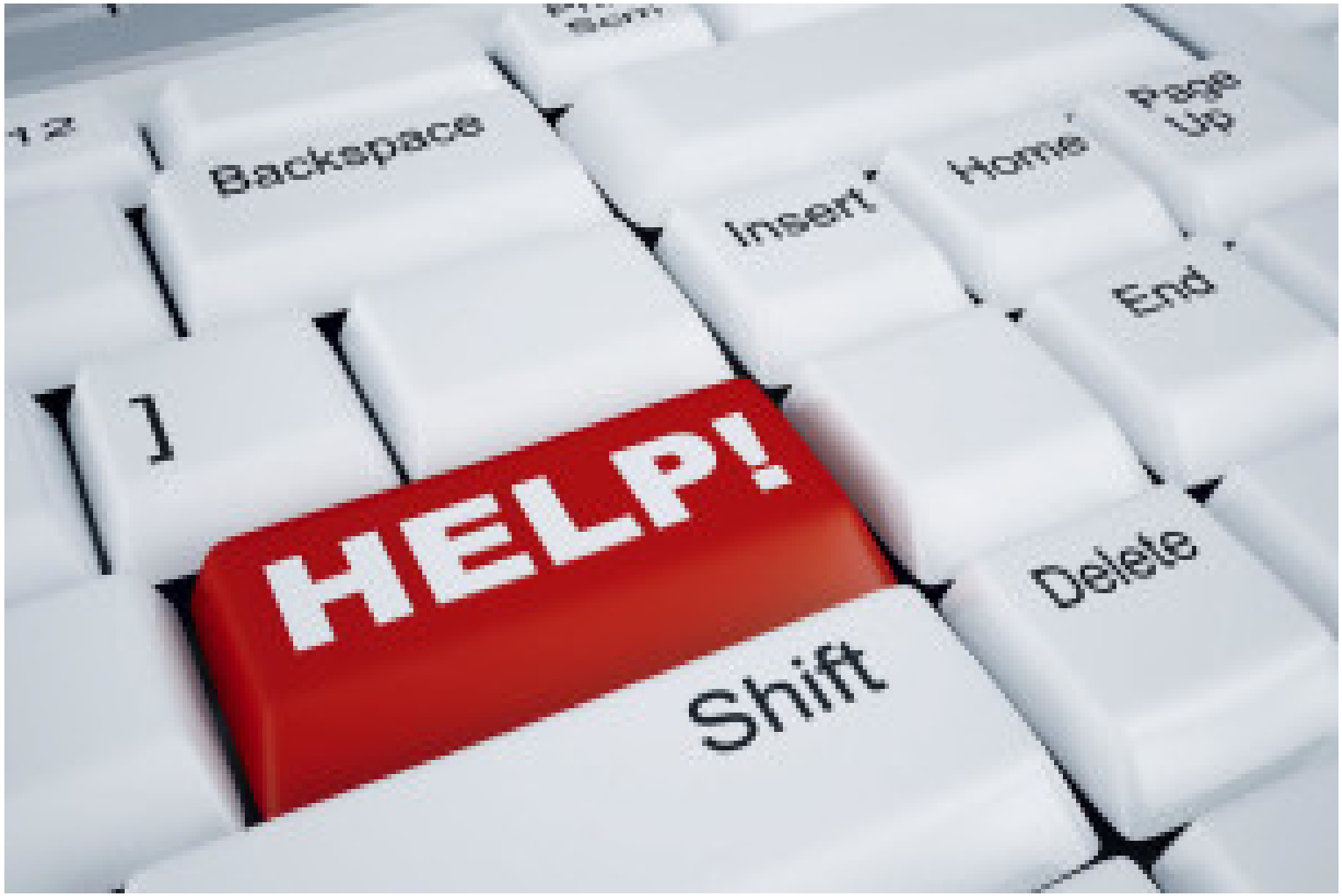
(67 FR 53252; *see also* FAQ available at https://www.hhs.gov/hipaa/for-professionals/faq/236/covered-entity-liable-for-action/index.html).

Requiring BA to Provide Documents or Audits of Its Compliance

- "The HIPAA Rules do not expressly require that a [BA] provide documentation of its security practices to or otherwise allow a customer to audit its security practices. "
- "However, customers may require from a [BA] (through the BAA, service level agreement, or other documentation) additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities."

(https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html)

Additional Resources



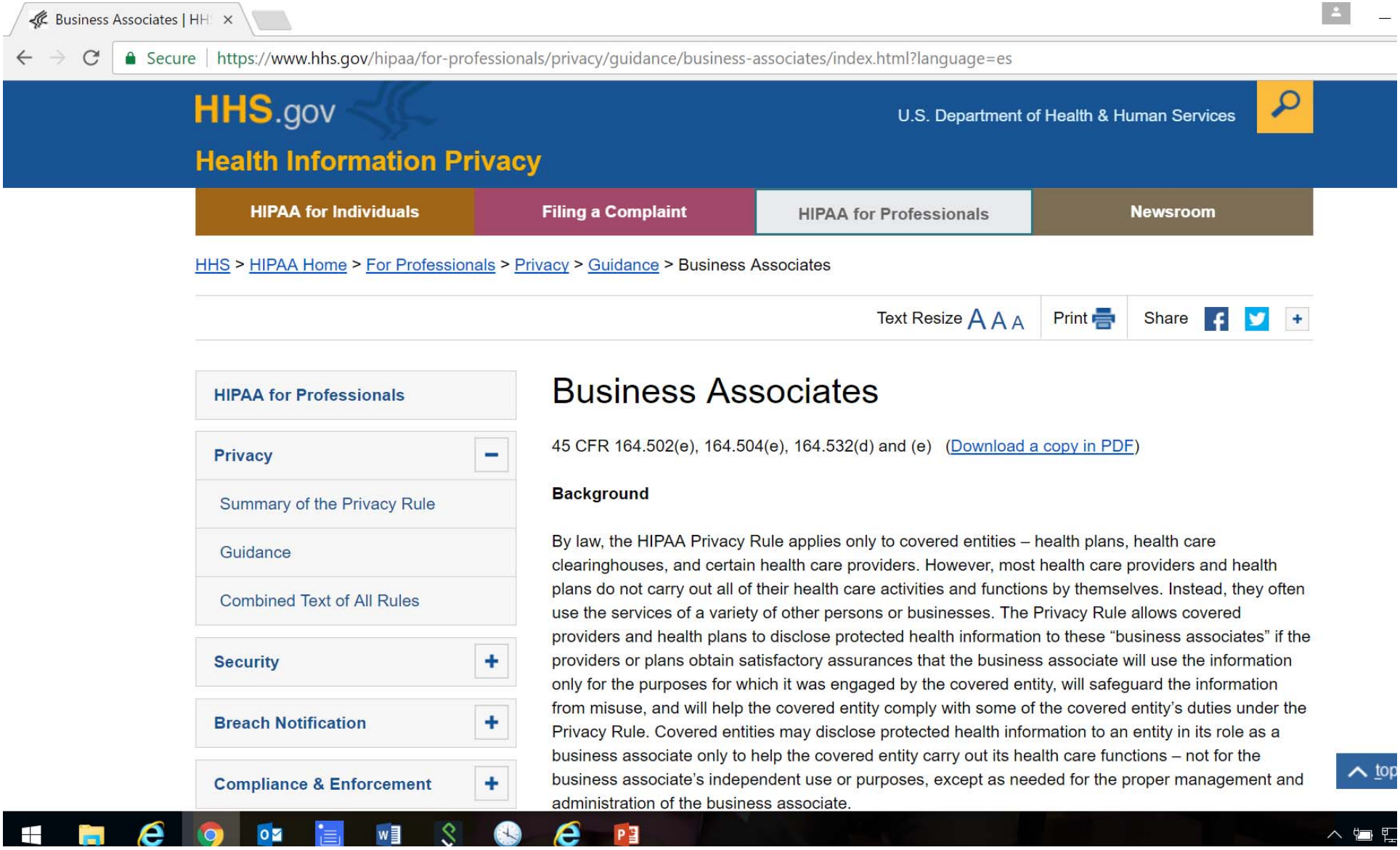
HOLLAND&HART

http://www.hhs.gov/hipaa

HIPAA Resources

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

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es



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

Healthcare | Holland & H

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

MENU HOLLAND&HART 70 YEARS EST. 1947

OVERVIEW

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS

Kim Stanger
Partner
Boise

Blaine Benard
Partner
Salt Lake City

HEALTH LAW BLOG
Access to previous webinar recordings, publications, and more.

The Healthcare
this sector now
stand ready to h

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

Clients We Serve

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

Oh Yes! IT'S FREE

Past Webinars
Publications

Most Popular Stories

Upcoming Holland & Hart Webinars

2/23 Responding to HIPAA Breaches

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

HOLLAND&HART

Questions?

Kim C. Stanger

Holland & Hart LLP

kcstanger@hollandhart.com

(208) 383-3913

HOLLAND&HART