

Checking Your HIPAA Business Associate Agreements



Kim C. Stanger

(2/19)

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



- **Who are business associates?**
- **What you must and should have in your business associate agreements (“BAAs”).**
- **Minimizing liability for business associate’s or subcontractor’s misconduct.**

Written Materials

- Written materials
 - .ppt slides
 - OCR, *Terms for Business Associate Agreement.*
 - OCR, *Guidance on HIPAA & Cloud Computing.*
 - Stanger, *Identifying Business Associates.*
 - Stanger, *Business Associate Decision Tree.*
 - Stanger, *Checklist for Business Associate Agreements.*
 - Stanger, *Minimizing Liability for Business Associate Misconduct.*
 - 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.

Why you should care about HIPAA and business associates



Covered Entities, Business Associates, and Subcontractors

Healthcare provider,
health plan, or
clearinghouse

Covered Entity
("CE")

BAA

Creates, receives,
maintains or transmits
PHI for covered entity

Business
Associate ("BA")

BAA

Creates, receives,
maintains or transmits
PHI for business
associate

Subcontractor

CE / BA
responsible
for BAA

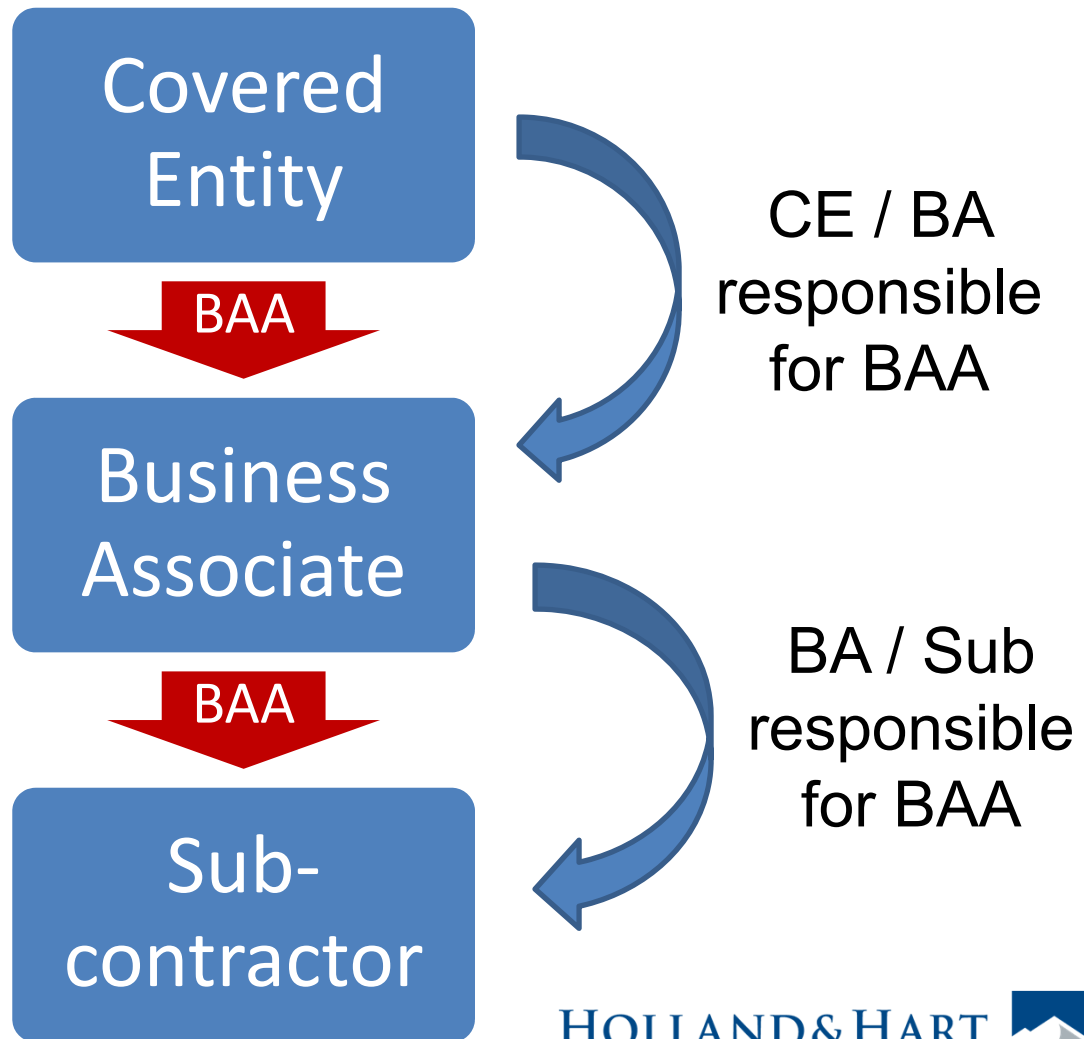
BA / Sub
responsible
for BAA

HOLLAND & HART^{LLP}



CEs, BAs, and Subcontractors

“[CEs] must ensure that they obtain satisfactory assurances required by the Rules from their [BAs], and [BAs] must do the same with regard to subcontractors, and so on, no matter how far ‘down the chain’ the information flows.” (78 FR 5574)



HIPAA Civil Penalties

(as modified by recent inflation adjustment)

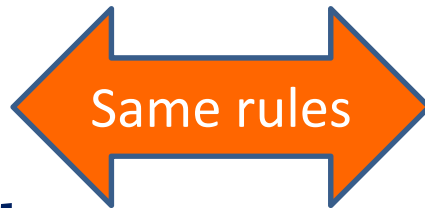
Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none">• \$112 to \$55,910 per violation• Up to \$1,667,299 per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Violation due to reasonable cause	<ul style="list-style-type: none">• \$1,118 to \$55,910 per violation• Up to \$1,667,299 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">• \$11,182 to \$55,910 per violation• Up to \$1,667,299 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 \$55,910 per violation• Up to \$1,667,299 per type per year• Penalty is mandatory

(45 CFR 160.404; see also 74 FR 56127)

Additional Consequences

- **State attorney general may bring lawsuit.**
 - \$25,000 fine per violation + fees and costs
- **Individuals may recover percentage of penalties.**
 - Still waiting on implementing regulations.
- **Must sanction workforce members who violate HIPAA.**
- **Must self-report breaches of unsecured protected health info (“PHI”).**
 - To affected individuals.
 - To HHS.
 - To media if breach involves > 500 persons.
- **Possibility of private lawsuit.**
 - No private cause of action under HIPAA, but HIPAA may be used as standard of care.

**CE Liability
for BA's
Misconduct**



**BA Liability for
Sub's
Misconduct**

Liability for Business Associate Misconduct

Under HIPAA, CE may be subject to penalties for BA's violations if:

- **CE knows of misconduct and fails to take appropriate action.**
- **BA is agent of CE.**
- **CE delegates duty to BA.**
- **CE fails to implement BAA.**

Other bases of liability

- **Contract**
- **State law, e.g.,**
 - Statutes
 - Licensing regulations
 - Common law agency
 - Express agency
 - Respondeat superior
 - Apparent authority
 - Joint and several liability for “acting in concert”
 - Others?

Liability for BA Conduct: Failure to Stop Misconduct

“(ii) A [CE] is not in compliance with [HIPAA], if the [CE] knew of a pattern of activity or practice of the [BA] that constituted a material breach or violation of the [BA]'s obligation under the contract or other arrangement, **unless the [CE] took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.**

“(iii) A [BA] is not in compliance with [HIPAA], if the [BA] knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, **unless the [BA] took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.**”

(45 CFR 164.504(e)(1), emphasis added)

Liability for BA Conduct: Agency Relationship

“Violation attributed to a covered entity or business associate.

“(1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the **act or omission of any agent** of the covered entity, including a workforce member or business associate, **acting within the scope of the agency**.

“(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the **act or omission of any agent** of the business associate, including a workforce member or subcontractor, **acting within the scope of the agency.**”

(45 CFR 160.402(c))

Workforce v. BA

Workforce

- “[E]mployees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is **under the direct control** of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.” (45 CFR 160.103)

Business Associate

- “Other than in the capacity of a member of the workforce of such covered entity or arrangement, **creates, receives, maintains, or transmits protected health information** for a function or activity regulated by [HIPAA].” (45 CFR 160.103)

Liability for BA Conduct: Delegated Duty

- BAA must contain following term:
 - “To the extent the [BA] is to carry out a [CE]'s obligation [under HIPAA], comply with the requirements [of HIPAA] that apply to the [CE] in the performance of such obligation.” (45 CFR 164.504(e)(2)(ii)(H))
- “[W]here a [CE] or [BA] has delegated out an obligation under the HIPAA Rules, ... a [CE] or [BA] would remain liable for penalties for the failure of its [BA] to perform the obligation on the [CE] or [BA]’s behalf.” (78 FR 5580; *see also* 75 FR 40879)

Liability for BA Conduct: Failure to Implement BAA

- “If a [CE] fails to comply with the [BA] provisions in the Privacy and Security Rules, such as by [1] not entering into the requisite contracts or arrangements, or [2] by not taking reasonable steps to cure a breach or end a violation that is known to the [CE], the [CE] may be liable for the actions of a [BA] agent.” (71 FR 8403, emphasis added)
- CE may be liable even if there is no agency relationship.

Recent OCR settlements based in whole or part on failure to have BAA

Date	Conduct	Penalty
12/18	Health system failed to have BAA with contractor that maintained ePHI	\$3,000,000
12/18	Hospital failed to have BAA with web-based vendor	\$111,400
12/18	Hospitalist group failed to enter BAA with billing company	\$500,000
12/17	Cancer care center failed to enter BAAs with vendors	\$2,300,000
4/17	Pediatric clinics failed to enter BAAs with file storage company	\$31,000
8/16	Health network failed to enter BAAs	\$5,500,000
7/16	Medical university failed to obtain BAA with cloud-based storage vendor	\$2,700,000
4/16	Radiology group failed to have BAA; x-rays left by vendor	\$750,000
3/16	Health system failed to have BAA; laptop stolen from care of BA's employee	\$1,550,000

Civil Penalties

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 condition of the patient. The medical conditions on the "checklist" include three mental health conditions (depression, bipolar disorder and schizophrenia); HIV; lung conditions like asthma; heart disease like high blood pressure and chronic heart failure; neurological diseases like Parkinson's and seizure disorders; and metabolic

HOLLAND & HART^{LLP}



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?



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 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)

Identify BAs

- **Business associates you may be missing:**
 - **Data storage companies, including cloud service providers.**
 - See OCR Guidance on Cloud Service Providers, available at <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>.
 - **Data processing or management companies**
 - **Document destruction companies**
 - **Health information exchange**
 - **EHR vendor**
 - **E-prescribing gateways**
 - **Software vendor or IT support**
 - **Vendors of equipment or services**
 - **Medical device manufacturers**



Identify BAs

- **Business associates you may be missing:**
 - Management company
 - Billing company
 - Answering service
 - Transcription service
 - Interpreter or translator if contracted by CE
 - Consultant
 - Auditor
 - Marketing or public relations firm
 - Accountant
 - Lawyer
 - Malpractice carrier
 - Collection agency if performing services for CE



Identify BAs

- **Business associates you may be missing:**
 - Third party administrator
 - Accreditation organization
 - Patient safety organization
 - State or national industry association that pro
 - Peer reviewers who review records
 - Medical directors
 - Med staff members providing training
 - Med staff members providing admin
 - Others?



Unless workforce
or part of organized
health care
arrangement
("OHCA")

Not BAs

- **Workforce members.**
 - “[E]mployees, volunteers, trainees, and other persons ... under the direct control of [CE].”
- **Persons who do not create, receive, maintain or transmit PHI as part of their job duties for CE.**
 - Janitors, Fed-Ex, plumber, electrician, and others whose job duties do not require access to PHI; access to PHI is incidental.
- **Members of organized health care arrangement.**
 - “A clinically integrated care setting in which individuals typically receive health care from more than one health care provider” (e.g., hospital and medical staff).
 - “[A]n organized system of health care ... in which the participating covered entities engage in joint utilization review, quality improvement, or payment activities (e.g., provider networks).”

Not BAs

- **Other health care providers with respect to disclosures concerning the treatment of the individual.**
 - Other doctors, hospitals, labs, therapists, etc. providing treatment.
- **Entities who are mere “conduits” for PHI.**
 - Internet service providers, phone companies, postal service, etc., who transmit but do not maintain or regularly access PHI.
- **Entities acting on their own behalf or on behalf of patient.**
 - Payers, banks, researchers, patient advocate, etc.
- **Entities performing management or admin functions for BAs.**
 - Services not performed on behalf of CE.
- **Government agencies performing their required functions.**

Identify BAs: Suggestions

- **Educate internal personnel re need for BAAs, e.g.,**
 - Administration
 - Medical records, information management, etc.
 - Financial services, accounting, and accounts payable
 - Marketing
 - Medicals staff services
 - Others who may contract with vendors who access PHI
- **Periodically review or audit list of BAs**
 - Review accounts payable
- **Include BAs and BAAs in periodic risk assessment**
 - Document assessment

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 if access, create, have e-PHI.
 - 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

Evaluating BA

- **Beware doing business with BA if you know they are not going to comply.**
 - E.g., small unsophisticated BAs.
 - Possible “willful neglect” if know they won’t comply.
- **Remember: must take appropriate steps to end violation if have “substantial and credible evidence of a violation.”** (45 CFR 164.504(e)(1); 65 FR 82505).

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.**

To BAA or Not to BAA

Covered Entities

- When in doubt, require BAA.
- May use data use agreement if appropriate.
- If no BAA, require confidentiality agreement.
 - Members of workforce
 - Contractors or others with incidental access to PHI but who are not BAs.

Business Associates

- Avoid BAA if you are not a BA.
- Make BAA conditional on status as BA.
- Consider alternative confidentiality agreement.

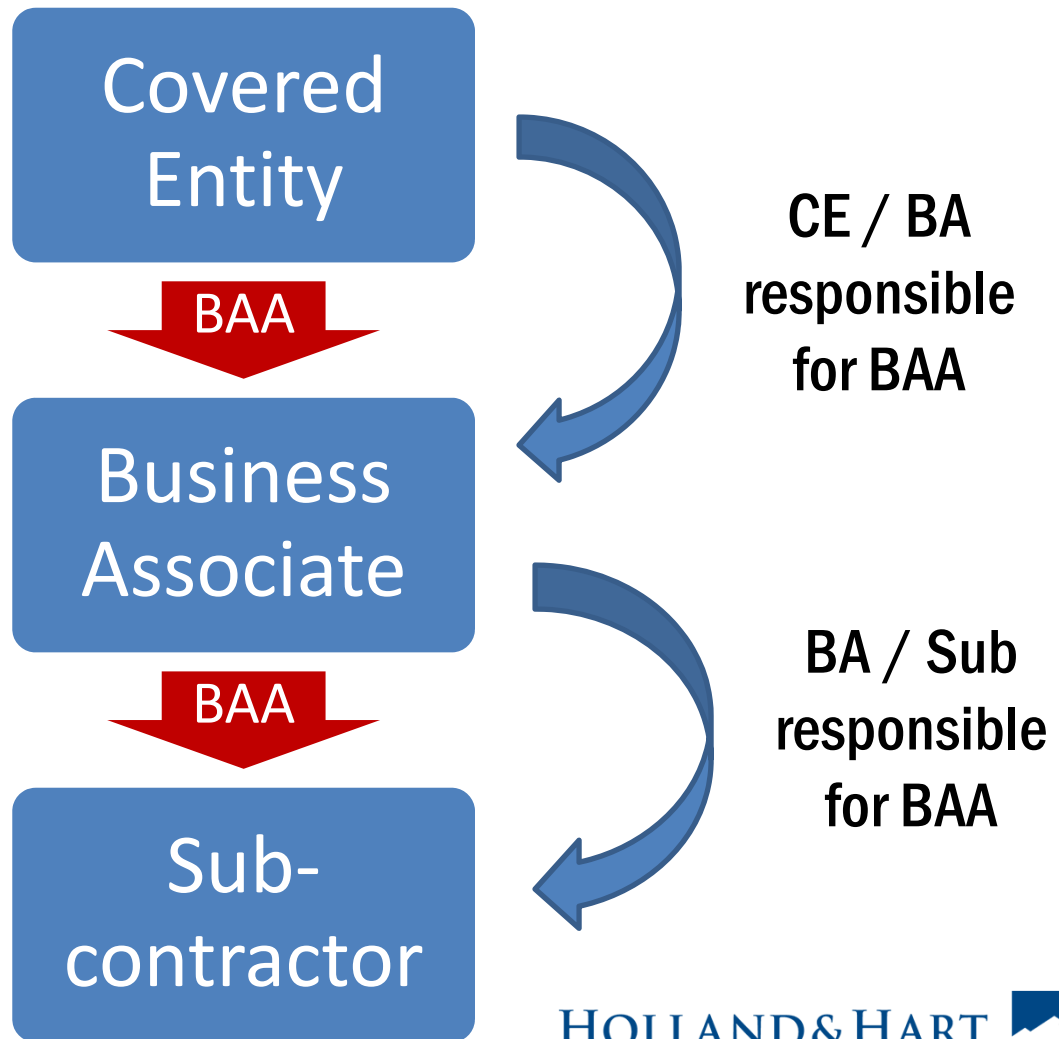
BAA: Required Terms

- **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.

(45 CFR 164.502(e) and 164.504(e))

BAA: Required Terms

“[E]ach agreement in the [BA] chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures.” (78 FR 5601)



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.

(45 CFR 164.502(e) and 164.504(e))

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.**

(45 CFR 164.502(e) and 164.504(e))

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.

(45 CFR 164.502(e) and 164.504(e))

BAA: Required Terms

- If covered entity delegates its functions to business associate, comply with HIPAA as to those functions.
 - Required by Omnibus Rule in 2013.
- 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.

(45 CFR 164.502(e) and 164.504(e))

BAA: Required Terms

A settlement illustra x

wayback.archive-it.org/3926/20170127192420/https://www.hhs.gov/about/news/2016/09/23/hipaa-settlement-illustrates-importance-of-revi...

HHS.gov U.S. Department of Health & Human Services

About HHS Programs & Services Grants & Contracts Laws & Regulations

Text Resize **A A A** Print Share   +

FOR IMMEDIATE RELEASE
September 23, 2016

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

Provider pays \$400,000 due to failure to update BAAs to include terms required by Omnibus Rule

HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements

Care New England Health System (CNE), on behalf of each of the covered entities under its common ownership or control, has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. The settlement includes a monetary payment of \$400,000 and a comprehensive corrective action plan. CNE provides centralized corporate support for its subsidiary affiliated covered entities, which include a number of hospitals and health care providers in Massachusetts and Rhode Island. These functions include, but are not limited to, finance, human resources, information services and technical support, insurance, compliance and

 [top](#)

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

HIPAA for Professionals

Privacy



Security



Breach Notification



Compliance & Enforcement



Special Topics



Patient Safety



Covered Entities & Business Associates



Business Associates

Business Associate Contracts

Training & Resources

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 workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity 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 health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to

BAA: Pro-Covered Entity Terms

- Covered entities may want to add these terms:
 - Business associate must report or act within x days, e.g., within 5 business days.
 - Business associate must implement policies to maintain privacy.
 - Business associate must encrypt or implement other safeguards to protect ePHI.
 - Business associate must carry acceptable data breach insurance.
 - Appropriate policy limits.
 - Appropriate scope of coverage.
 - Name covered entity as additional insured.

* *Business associate may want these in subcontracts.*

BAA: Pro-Covered Entity Terms

- Covered entities may want to add these terms (cont'd):
 - 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 is liable for acts of subcontractors.
 - Allow termination of underlying agreement if BAA violated.
 - 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 not excluded from Medicare.

* *Business associate may want these in subcontracts.*

BAA: Pro-Covered Entity Terms

- Beware retaining too much control of business associate, e.g.,
 - Review of policies or safeguards
 - Covered entity directs business associate actions
 - Covered entity must approve business associate's actions
 - Others?
- May make the business associate your agent.
- May be liable for business associate's acts or omissions.

BAA: Pro-Covered Entity Terms

- Beware delegating functions to business associate, e.g.,
 - Providing access to PHI
 - Amending PHI
 - Accounting for PHI
 - Mitigating breaches
 - Breach reporting
 - Security rule compliance
 - Others?
- May be liable for business associate's acts or omissions.

BAA: Pro-BA Terms

- **Business associates and subs probably want to add these:**
 - **Condition obligations on status as business associate.**
 - **Covered entity will not disclose PHI unless necessary.**
 - **Covered entity will not request action that violates HIPAA.**
 - **Covered entity has obtained necessary authorizations or consents.**
 - **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 that may affect business associate.**
 - **Covered entity will reimburse business associate for additional costs.**

BAA: Pro-BA Terms

- **Business associates and subs probably want to add these (cont'd):**
 - Blanket reporting for insignificant 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; business associate is not liable for their conduct.
 - Mutual indemnification.
 - Limitation or cap on damages, e.g.,
 - Dollar amount
 - Costs under contract
 - Available insurance
 - Others?

BAA Negotiation

It comes down to bargaining power...



BAA: Summary

- **Covered entities: when in doubt, demand BAA.**
- **Business associates: 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 business associate, 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.

Educate BAA re Duties

- **Appropriate BAA terms.**
 - May want to specify duties in BAA.
- **Additional educational materials, e.g.,**
 - Letter explaining BA duties and penalties for noncompliance.
 - <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>
 - Stanger, *Complying with HIPAA: A Checklist for Business Associates*, available at <https://www.hollandhart.com/checklist-for-business-associates>
- **Beware undertaking duty to train or supervise BA unless willing to assume liability.**

Monitor or Audit BAs?

os://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue-4.pdf

May 3, 2016

OCR Cyber-Awareness Monthly Update

April 2016 Topic: Is Your Business Associate Prepared for a Security Incident?



Despite the requirements of HIPAA, not only do a large percentage of covered entities believe they will not be notified of security breaches or cyberattacks by their business associates, they also think it is difficult to manage security incidents involving business associates, and impossible to determine if data safeguards

Monitoring BAs

- “Covered entities and business associates should train workforce members on incident reporting and may wish to conduct security audits and assessments to evaluate the business associates’ or subcontractors’ security and privacy practices. If not, ePHI or the systems that contains ePHI may be at significant risk.”

(OCR Cyber-Awareness Monthly Update dated 5/3/16), available at <https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue-4.pdf>)

- Sparked consultants’ advice to audit, assess, and/or monitor BA’s privacy practices.

Monitoring BAs

- **No obligation under HIPAA to actively monitor or ensure business associate's compliance.**
 - As originally proposed, privacy rule would have required covered entity to take reasonable steps to ensure BA compliance.
 - Final rule eliminated that standard; instead, under final rule, the covered entity must:
 - Execute BAAs.
 - Take appropriate action if know that BA is violating HIPAA.

(65 FR 82505 and 82641)

Monitoring BAs

- “Is a covered entity ... required to monitor the actions of its business associates?”
- “Answer: No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract....”

(OCR FAQ 12/19/2002, emphasis added; see also 65 FR 82505 and 82641)

BA Not Required to Subject Itself to Monitoring or Review

- “Do the HIPAA Rules require [Cloud Service Providers] that are [BAs] to provide documentation, or allow auditing, of their security practices by their customers who are covered entities or business associates?”
- “Answer: No. ... **The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices to or otherwise allow a customer to audit its security practices.** However, customers may require from a CSP (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.”

Monitoring BAs

Pros

- May help ensure BA acts appropriately.
- May help avoid “willful neglect” if BA acts improperly.
- May mitigate liability if BA does not act appropriately.

Cons

- Cost and resources.
- Monitoring → control → agent → vicarious liability.
- If assume duty, may be liable for failing to exercise reasonable care in fulfilling duty.
 - You should have known → you should have acted.

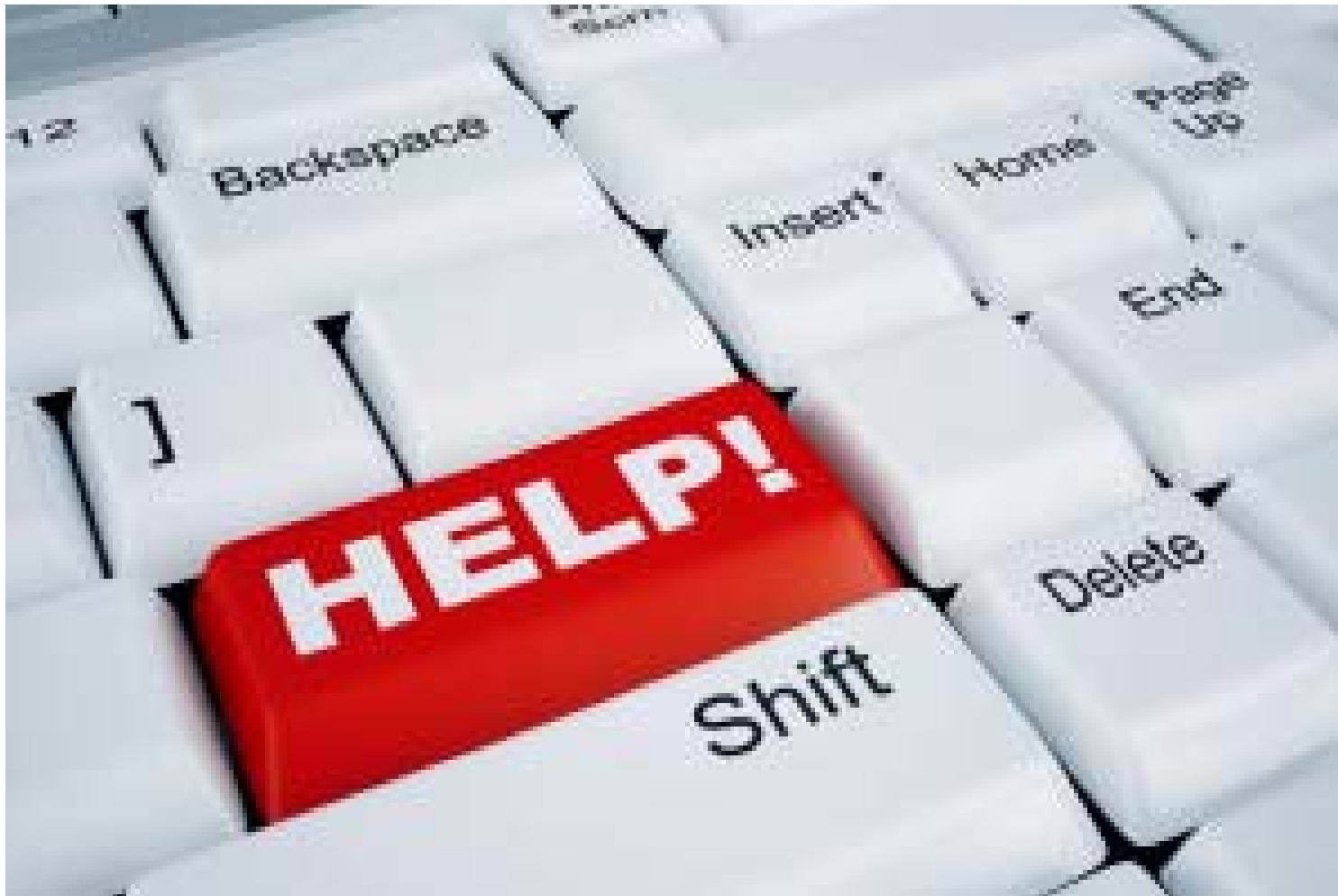
Monitoring BAs



Cons

- Might uncover problems that you would not otherwise be obligated to address...
- Ignorance is bliss.

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](#).
- [View the Combined Regulation Text](#) (as of March 2013). This is an unofficial version that presents all the HIPAA regulatory standards in one document. The official version of all federal regulations is published in the Code of Federal Regulations (CFR). View the official versions at 45 C.F.R. [Part 160](#), [Part 162](#), and [Part 164](#).

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.hollandhart.com/healthcare#overview>

EXCELLENCE IN LEGAL SERVICE


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 Industry
This sector now stands ready to handle
Issues such as rising costs, regulatory changes, and innovations in health care are on the minds of many of our attorneys. We are prepared to help you navigate these opportunities that are available.

Clients We Serve

- Hospitals
- Individual medical practices
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- Health information exchanges (HIEs)
- Practice managers and administrators
- Veterinary service providers and facilities
- Independent practice associations (IPAs)
- Imaging centers
- Ambulatory surgery centers
- Medical device and life science companies

Oh Yes! IT'S FREE

Past Webinars Publications

Questions?



Kim C. Stanger
Holland & Hart LLP
[kcstanger@hollandhart.](mailto:kcstanger@hollandhart.com)
[com](mailto:kcstanger@hollandhart.com)
(208) 383-3913