Health Insurance Portability and Accountability Act (HIPAA) California CLE: 2015

Edward Dailo, Esq.
Corporate Attorney

Ruben Medina, Esq.
General Counsel

second IMAGE NATIONAL

Introduction

Ruben Medina, Esq., General Counsel
Second Image National

Mr. Medina oversees all legal matters relating to Second Image National's daily business across the country. He is also responsible for Second Image National's compliance with State and Federal Regulation as the company's Compliance Officer. Mr. Medina received his Juris Doctorate from Southwestern Law School and Bachelors from the University of California, Irvine. He is certified as a HIPAA Professional and in the field of Health Care Privacy/Security. Prior to his role as General Counsel, Mr. Medina worked for a private national civil litigation foundation dealing with a variety of healthcare and civil rights actions. Mr. Medina is admitted to practice law in California, District of Columbia (D.C.), and Texas.

Phone: 800-220-7477 | Email: Ruben.Medina@secondimage.com

second IMAGE NATIONAL

Introduction

Edward P. Dailo, Esq., Corporate Attorney
Second Image National

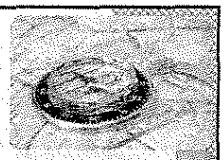
Mr. Dailo received his B.A. degree in International Relations and minor in Business from the USC in 2006. He received his J.D. from the University of La Verne College of Law in 2011. Mr. Dailo is also a HIPAA Certified Professional.

Prior to Second Image National, Mr. Dailo worked for the Riverside City Attorney's Office and the Neighborhood Legal Services of Los Angeles County. He has served as president for the USC Alumni Club of the Inland Empire, and maintains an active role with the La Verne College of Law Alumni Committee, Philippine American Bar Association (PABA), Asian Pacific American Bar Association (APABA), Los Angeles County Bar Association (LACBA), and Western San Bernardino County Bar Association (WSBCBA).

second IMAGE NATIONAL

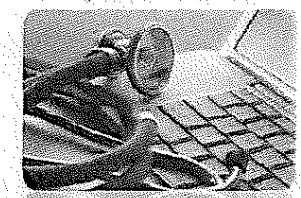
Phone: 909-909-3899 | Email: Edward.Dailo@secondimage.com

Road Map



1. HIPAA Overview
2. HIPAA By The Numbers
3. Does HIPAA apply to me?
4. Compliance under HIPAA
5. Areas of Risk
6. Business Associate Agreements
7. Breaches: Unsecured Protected Health Information

1. HIPAA Overview



HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

- Also known as the Kennedy-Kassembaum Bill
- Signed by President Clinton in 1996.

HIPAA

Main purposes:

1. To improve the portability and continuity of health insurance coverage in the group and individual markets,
2. To combat waste, fraud, and abuse in health insurance and health care delivery,
3. To promote the use of medical savings accounts,
4. To improve access to long-term care services and coverage,
5. To simplify the administration of health insurance.

HIPAA: Final Omnibus Rule (March 2013)

- HIPAA extends to subcontractors and vendors storing PHI for Covered Entities and Business Associates. 45 CFR 160.103(3)(iii).
- Harsher penalties for privacy and security violations.
- Changes the determination of what is considered a breach.
- Changes to Business Associate Agreements.

HHS office for Civil Rights

- Director Leon Rodriguez, HHS Office for Civil Rights
  - "This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented."
  - "These changes not only greatly **enhance a patient's privacy rights and protections**, but also strengthen the ability of my office to **vigorously enforce the HIPAA privacy and security protections**, regardless of whether the information is being held by a health plan, a health care provider, or **one of their business associates**." Director Leon Rodriguez, HHS Office for Civil Rights.

HHS.gov Press Release 1.17.2013. http://www.hhs.gov/news/press/2013pres/01/20130117b.html

HIPAA: PHI

- Protected Health Information (PHI) – any individually identifiable information created or received by a CE, regardless of the media form it is/was stored.
  - Ex. Information your health care providers put into your medical records
  - Ex. Conversations about medical care and treatment
  - Ex. Billing information

HIPAA: Privacy

Privacy Rule defines and limits the circumstances in which PHI may be used or disclosed.

- To Individuals/Representatives (Authorizations)
- As required by Law (Subpoena, Court Order)
- Incidental Use & Disclosure (Minimum Necessary Rule)
- To HHS (Investigations)

HIPAA: Security

Security Rule – intends to ensure security safeguards are adopted to protect PHI which may be at risk.

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

Reasonable and Appropriate Standard

Per ecFirst, Confidentiality, Integrity, and Availability are the components of security.

2. HIPAA By the Numbers

Civil Penalties

	For Violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	Up to $100 per violation	$100 to $50,000
Calendar Year Cap	$25,000	$1,500,000

Criminal Penalties

- $50,000 and up to one year imprisonment
- $100,000 and up to five years imprisonment
- $ 250,000 and up to ten years imprisonment

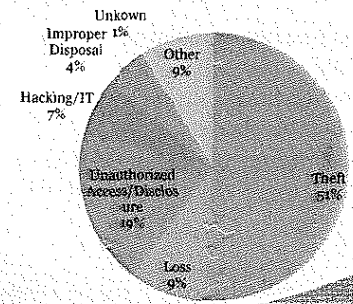
Breach Breakdown

Sept 2009 – Feb 27, 2015

- ~1,144 reports of breach affecting 500+ individuals
  - 60% - Theft and Loss
  - 32% - Laptops and portable storage devices
  - 22% - Paper records
- ~157,000 reports of breaches affecting <500 individuals

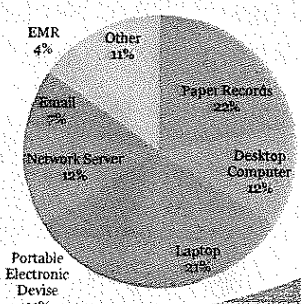
Source: Jocelyn Samuels Director of HHS Office of Civil Rights – 23rd National HIPAA Summit March 16, 2015

500+ Breaches by Type of Breach as of 2/2015



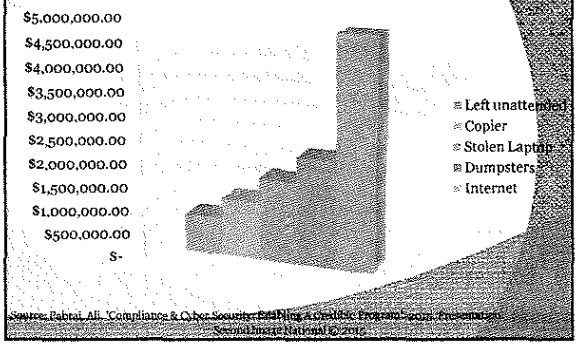
Source: Jocelyn Samuels Director of HHS Office of Civil Rights – 23rd National HIPAA Summit March 16, 2015

500+ Breaches by Location of Breach as of 2/2015



Source: Jocelyn Samuels, HHS Office for Civil Rights – Keynote Address 23rd National HIPAA Summit March 16, 2015

Risks to Business



Source: Pabrai, Ali. 'Compliance & Cyber Security: Building a Credible Program' 2015. Presentation.
Second Image National © 2015

Emerging HIPAA Security Areas of Concern...

- ID Theft and Medical ID Theft on rise
  - As more healthcare data is digitized
  - Full set of ID info: $10-150 (med records will have demo, fin, and med)
  - SSN: $.50-$2
  - Stolen Credit Card: $.05-$5
  - Set of Medicare ID numbers for 10 beneficiaries found online by security company RedJack was being sold for 22 bitcoins, or ~$4,700
  - Websites offers such data tend to have names that end with .su or .so, as opposed to .com or .org. Some sites for criminal sales feature online ratings systems, similar to Yelp, that let the buyer know if the seller is legit (5* is top rating)

Source: John Parmigiani, 23rd Annual HIPAA Summit March 16, 2015
Second Image National © 2015

Emerging HIPAA Security Areas of Concern... (Pt 2)

- Major market is part of a kit for illegal immigrants to establish a fake identity and receive healthcare in US
- Sold to individuals without insurance who are in need of elective surgeries or other expensive treatments, especially as the cost of healthcare is rising and the uninsured population is also increasing
- Used by criminal providers for submitting fraudulent claims

Source: John Parmigiani, 23rd Annual HIPAA Summit March 16, 2015
Second Image National © 2015

Stats on workforce

- Workforce is biggest security threat
  - 90% of malware requires a human interaction to infect
  - 33% of workers use same password for work and personal devices
  - 35% clicked on email links from unknown senders
  - 59% stored work info on cloud
  - 56% of employees don't receive any data security awareness training (some training isn't effective)

Source: Daniel J. Solove – 20th National HIPAA Summit, March 2012
Second Image National © 2015

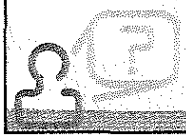
3. Does HIPAA' Security Rule apply to me?

Second Image National © 2015

Does HIPAA's Security Rule apply to me?

Can you be categorized in any of the following?

1. Covered Entities
2. Business Associates
3. Subcontractors who stores ePHI for a Covered Entity or Business Associate.



Second Image National © 2015

Covered Entities

Covered entity: (45 CFR § 160.103)

(1) A health plan.

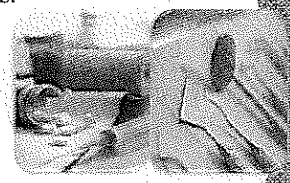
(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered Entities

Healthcare Providers:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies



*If they transmit information in electronic form.

Business Associate

Business Associate: (45 CFR § 160.103)

A person who is not a member of the Covered Entities Workforce and

- Arranges, creates, receives, maintains, or transmits protected health information (PHI),

or

- Provides, ***legal***, actuarial, accounting, consulting, data, aggregation, management, administration, accreditation, or financial services to or such covered entity and where ***the services involve the disclosure of protected health information.***

BA: Law Firms

Law Firm employees (attorneys, paralegals, legal assistants) are considered the work force of a Business Associates if they transmit, disclose, receive, or maintain protected health information in the course of representing a Covered Entity or Business Associate.

- Examples:
  - Authorizations for Medical Records
  - Court Orders/Qualified Protective Orders
  - Subpoena for Medical Records
  - Transmission of Medical Records to Experts/Claim Adjusters

Subcontractor (Sub-K)

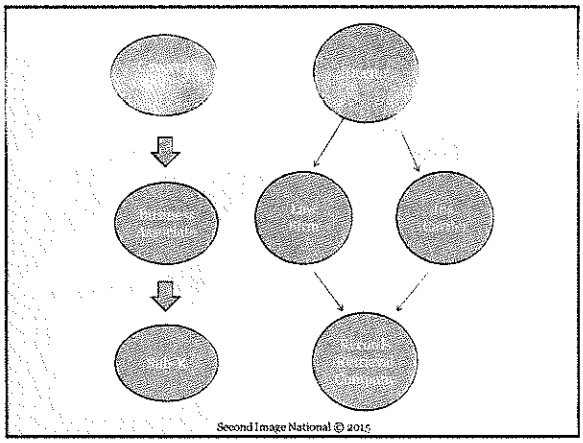
Subcontractor: (45 CFR 160.103)

- A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.
- Also defined as Business Associates under HIPAA.

Sub-K:Support Services

Support Services are those that assist the Business Associate in maintaining, transmitting, disposing, or storing protected health information.

- Examples:
  - Record Retrieval Company
  - Court Reporting Company
  - Record Disposal Company
  - Copy Machine Vendor
  - IT (outsourcing)



Who is and is not covered?

Covered	Not Covered
1. Health Plans 2. Most Health Care Providers 3. Health Care Clearinghouses	1. Life insurers 2. Employers 3. Workers Compensation Carriers 4. Most Schools & School Districts 5. Many State Agencies like child protective service agencies 6. Most law enforcement agencies 7. Many municipal Offices

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

4.Compliance Under HIPAA's Security Rule

HIPAA compliance

Compliance

Under the HIPAA's Security Rule, Covered Entities/Business Associates/Subcontractors must:

- Ensure confidentiality, integrity and availability of electronic protected health information (ePHI)
- Protect against anticipated threats hazards.
- Protect against unpermitted uses or disclosures of ePHI
- Ensure compliance from your workforce

45 CFR 164.306(a)(1-4)

Compliance

HIPAA Security Rule allows CE/BA/Sub-K to implement measures that ***reasonably*** and ***appropriately*** meet the requirements of the rule.

Factors to consider for ***reasonable*** and ***appropriate***:

1. Size, complexity, and capabilities,
2. Technical Infrastructure, hardware and software,
3. Costs of security measures, and
4. Probability of potential risks.

45 CFR 164.306(b)(1)

Compliance

CE/BA/Sub-k must have in place ***administrative***, ***physical***, and ***technical*** safeguard in accordance with the Security Rule.

Compliance

The Security Rule contains ***required*** and ***addressable*** measures for each safeguard.

- ***Required*** measures means they **must** be implemented.
- ***Addressable*** measures mean they **must be assessed** whether its reasonable and appropriate for the entity to implement.

Compliance: Admin.

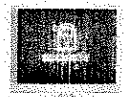
Required	Addressable
•Risk Analysis, •Risk Management, •Sanction Policy, •Information System Activity Review, •Isolation of Clearing Houses, •Security Response and Reporting, •Data back-up plan, •Disaster Recovery Plan, and •Emergency Mode Operation plan.	•Authorization/Supervision •Workforce Clearance Procedures, •Termination Procedures, •Security Reminders, •Protection from Malicious Software, •Access Authorization, •Access establishment and modification, •Log-in monitoring, •Password Management, •Testing and Revision Procedures, •Application and Data Criticality Analysis.

Compliance: Physical

Required	Addressable
•Disposal •Media re-use.	•Contingency Operations, •Facility Security Plan, •Access Control and validation procedures, •Maintenance records, •Accountability, •Data back-up and storage.

Compliance: Tech

Required	Addressable
•Unique User Identification, •Emergency Access Procedures.	•Automatic Logoff, •Encryption and Decryption, •Mechanism to authenticate ePHI, •Integrity Controls, and



4. Areas of Risk

Risk Analysis

Assessment of Risk:

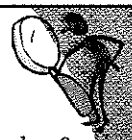
- Under HIPAA, you must make an assessment of the potential risks and vulnerabilities to ePHI.
  - Required under Administrative Safeguards.

Risk Analysis

Potential Risks:

1. Where is PHI and ePHI stored?
2. Who has access to ePHI? (attorneys, paralegals, legal assistants)
3. Is access limited to assignment/case or commingled with other records?
4. Do you track user access and use? (Accountability)

Risk Analysis



Potential Risks:

5. Do you have workstation security in place? (Auto-log off, Access based on user, viewable to unauthorized individuals/vendor, passwords)
6. Is there encryption of Mobile Devices/Laptops/USB drives/Tablets in place?
7. Is there a mobile device policy at place of employment? (Bring your own)

Risk Analysis

Potential Risks:

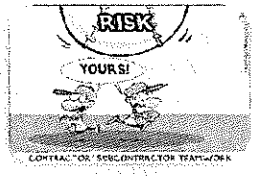
8. Do you have anti-virus software on your network and on computers?
9. Is there an accounting of all ePHI disclosed?
10. Are computer hard drives wiped of ePHI before they are disposed, sold, or moved to another department? (Xerox/Copy machines)

Risk Analysis

Potential Risks:

11. Do you have procedures in place to remove User access from an individual when they are no longer a member of the workforce?
12. Are there emergency access procedures for accessing ePHI?
13. Is there a Disaster Recovery plan in place?
14. Do you provide employee training on HIPAA compliance?

5. Business Associate Agreements



Business Associate Agreements

Who do I need this with?

- ❑Clients (Covered Entities)
- ❑Insurance Carriers (Business Associates)
- ❑Record Retrieval Companies
- ❑Deposition Officers
- ❑Expert Witnesses (Recommended)
- ❑Any vendor accessing PHI

BA Agreements

•Each party in chain needs a BAA from direct contractor

•BA must flow down applicable provisions from BAA to any sub-K whom BA **delegates a function, activity, or service (creating, receiving, maintaining, or transmitting PHI)**, other than as a BA workforce member.

Source: John Parmigiani. 23rd Annual HIPAA Summit. March 16, 2015

Business Associate Agreements

CE/BA's must have Business Associate Agreement in place with their business associates and/or subcontractors.

- ❑The BAA must contain the following:
  - Compliance with Privacy and Security Rules under HIPAA
  - Reporting of security incidents and breaches of unsecured ePHI
  - Breach Notification requirements

BA agreements (45 CFR 164.314)(a)(2)

Business Associate Agreements

Recommendations to request from BA/Sub-k for due diligence:

- ❑Third Party Audit of Vendor (SOC 1/ SOC 2/HIPAA)
- ❑Ability Audit Vendors Facility
- ❑Accountability Reports (user access)
- ❑Indemnification Clause

BA agreements (45 CFR 164.314)(a)(2)

6. Breach: Unsecured Protected Health Information

Breach

Breach (45 CFR 164.402)

- ❑Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by HIPAA] which compromises the security or privacy of the protected health information.

Breach

Presumption of a Breach unless CE/BA/Sub-K can demonstrate low probability that PHI was compromised.

- ❑Demonstrate by:
  - Identifying the nature of the PHI involved,
  - The unauthorized person who used PHI or to whom the disclosure was made to,
  - Whether PHI was actually acquired or viewed, and
  - Extent to which risk was mitigated.

Risk Assessment of Breach (45 CFR 164.402(2)(i-iv)

Breach

- Focus on the risk to the data, instead of the risk of harm to the individual
- Breach Analysis must be documented

Breach- Notification

If there is a breach of PHI, who do I notify?

- If 500 or less, you must notify each individual whose unsecured PHI has been accessed, acquired, used, or disclosed, no later than 60 calendar days after discovery of a breach.
- Must keep a log of breaches and at the end of the calendar year (no later than 60 days after) report to HHS.
- BAA, may have requirements that the Covered Entity do the report.

Notification of Individual (45 CFR 164.404)

Breach- Notification

If there is a breach of PHI relating to more than 500 individuals, who do I notify?

- Must notify prominent media outlets, no later than 60 calendar days after discovery of a breach.
- Additionally, must notify Secretary from HHS

Notification to the Media (45 CFR 164.406)

QUESTIONS?

Contact Information

- Edward Dailo, Esq.
  - Email: Edward.Dailo@secondimage.com
- Ruben Medina, Esq.
  - Email: Ruben.Medina@secondimage.com

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to

report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business

associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1.

    1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
    2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;
    3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
    4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and
    5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

**This information was provided by Business Associate Contracts, Sample Business Associate Agreement Provisions, Published January 25, 2013 by the Department of Health and Human Services at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html