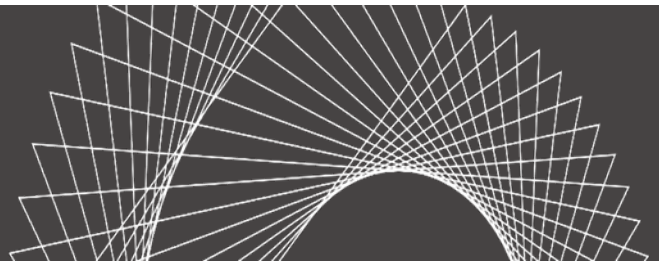
Buying a Breach: HIPAA Best Practices in M&A



Akin Gump
STRAUSS HAUER & FELD LLP

November 14, 2019

Jo-Ellyn Sakowitz Klein, J.D., CIPP/US

Managing Privacy and Data Security Risk in Business Deals

Appreciate the regulatory environment

Conduct reasonable diligence – ask the right questions at the outset

- Understand the data flows
- Be aware of regulatory pitfalls, starting with HIPAA risks
- Review documents material to HIPAA compliance
- Understand – and hold parties accountable for – their data practices

Careful contracting is key to managing privacy and cybersecurity risks in business deals

Regulatory Landscape in Which Deals Are Made

Regulatory Lay of the Land

U.S. Department of Health and Human Services, Office for Civil Rights (OCR)

- HIPAA – Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
- HIPAA and HITECH create a patchwork of policies addressing privacy, security, and breach notification, among other issues

Federal Trade Commission (FTC)

- Section 5 – privacy and security enforcement under authority to protect consumers against unfair and deceptive acts and practices
- Health Breach Notification Rule for Electronic Personal Health Records
- Internet of Things

Office of the National Coordinator for Health Information Technology (ONC)

Substance Abuse and Mental Health Services Administration (SAMHSA)

- Part 2 (42 CFR Part 2)

Food and Drug Administration (FDA)

State Attorneys General

A Time of Change

The California Consumer Privacy Act (CCPA)

The EU General Data Protection Regulation (GDPR)

HIPAA Overview

HIPAA is no longer new—so regulators expect compliance

- HIPAA was enacted in 1996 and was amended by HITECH in 2009
- HIPAA and HITECH have been implemented through rules generally taking effect in 2003 (privacy), 2005 (security), 2009 (breach notification) and 2013 (omnibus)

Changes to the HIPAA regime under HITECH and related regulations dramatically enhanced regulatory risks relating to data privacy and security:

- Extended reach to more entities
- Increased penalties
- New enforcement tools
- New audit mechanism
- New breach notification requirements
- Changes to privacy requirements

Who Must Contend with HIPAA?

Covered Entities

- HIPAA applies to covered entities (CE)—health plans, certain health care providers, and health care clearinghouses

Business Associates

- HIPAA business associates (BA) provide services, for or on behalf of covered entities, which involve HIPAA-protected information
- Must enter into a "Business Associate Agreement" and comply directly with much of HIPAA
- Business associates may only use PHI for the purposes for which it was disclosed to the business associate and otherwise in accordance with the terms of the agreement

What Information Is Protected?

PHI

- HIPAA mandates special protections for "protected health information" (PHI)
- PHI generally includes any information (including demographic information), whether oral or written, that:
  - Is created or received by a health care provider (such as a physician), health plan, employer, or health care clearinghouse;
  - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - Identifies, or could reasonably be expected to identify, the individual

Be aware that the nature and scope of information that is restricted under HIPAA is very broad

HIPAA Privacy Rule

The HIPAA Privacy Rule governs collection, use, and disclosure of PHI

General edict:

- A covered entity may not use or disclose PHI without authorization, unless that use or disclosure is otherwise permitted or required by HIPAA

Required uses and disclosures include:

- To an individual (or personal representative) exercising his or her individual rights of access, amendment or accounting
- To HHS for compliance

Permitted uses and disclosures include:

- “Incident to” another permitted use or disclosure
- For treatment, payment, or health care operations (TPO)
- “Limited data set” if pursuant to Data Use Agreement and for research, public health, or health care operations
- Public health purposes
- “Required by law”
- Law enforcement
- Pursuant to valid authorization

HIPAA-Compliant Authorization

Written authorization is generally required for non-routine disclosures of PHI, to the extent a HIPAA exception does not apply (e.g., marketing)

Mandatory elements:

- Meaningful description of the information to be used or disclosed
- Person, or class of persons, authorized to (i) make the requested use or disclosure and (ii) receive and use the PHI
- Description of each purpose of the requested use or disclosure
- Expiration date or event
- Signature of the individual and date (and a description of a personal representative's authority to act for the individual, if relevant)
- Right to revoke
- Ability or inability to apply conditions to the execution of the authorization
- Potential for redisclosure

Restriction on compound authorizations

Other relevant legal requirements

- State law
- Common Rule for research

HIPAA Privacy Rule – Key Concepts

Individual Rights

- Access
- Amendment
- Accounting
- Privacy protection

Personal Representative

- HIPAA personal representatives step into the shoes of the individual
- If under applicable law a person has authority to act on behalf of an individual who is an adult in making decisions related to health care, a covered entity must treat such person as a personal representative under HIPAA

Minimum Necessary

- Only use, disclose, or request the minimum amount of PHI needed to accomplish the intended purpose

Marketing

Sale of PHI

HIPAA Security Rule

Core goals of the HIPAA Security Rule

- Ensure the confidentiality, integrity, and availability of electronic PHI (ePHI) created, received, maintained, or transmitted by covered entities and business associates
- Protect against reasonably anticipated threats and hazards to the security or integrity of ePHI
- Protect against reasonably anticipated HIPAA Privacy Rule violations

Basic foundation for compliance

- Assessment and management of risk
- Reasonable and appropriate written policies and procedures
- Development and implementation of administrative, physical, and technical safeguards

HIPAA standards and implementation specifications

- Addressable (A) versus Required (R)
- Not a one-size-fits-all approach

Maintenance required

Organizational requirements

- Business Associate Agreements

Security Safeguards

Administrative Safeguards

- Security risk management process (including risk analysis and sanction policy)
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation
- Business Associate Agreements

Physical Safeguards

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls (including disposal)

Technical Safeguards

- Access control (including encryption and decryption)
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security (including encryption)

HHS Breach Notification Rule

Breach Notification Rule has been in effect since 2009, was modified in 2013, and may apply atop U.S. state breach notification laws

A "breach" is the unauthorized acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of that information, subject to limited exceptions

- Risk assessment involving four-factor test to determine if there is a low probability that the PHI has been compromised:
  - Nature of the PHI
  - Entity receiving the PHI
  - Whether the PHI was actually acquired or viewed
  - Extent to which risk to the PHI has been mitigated

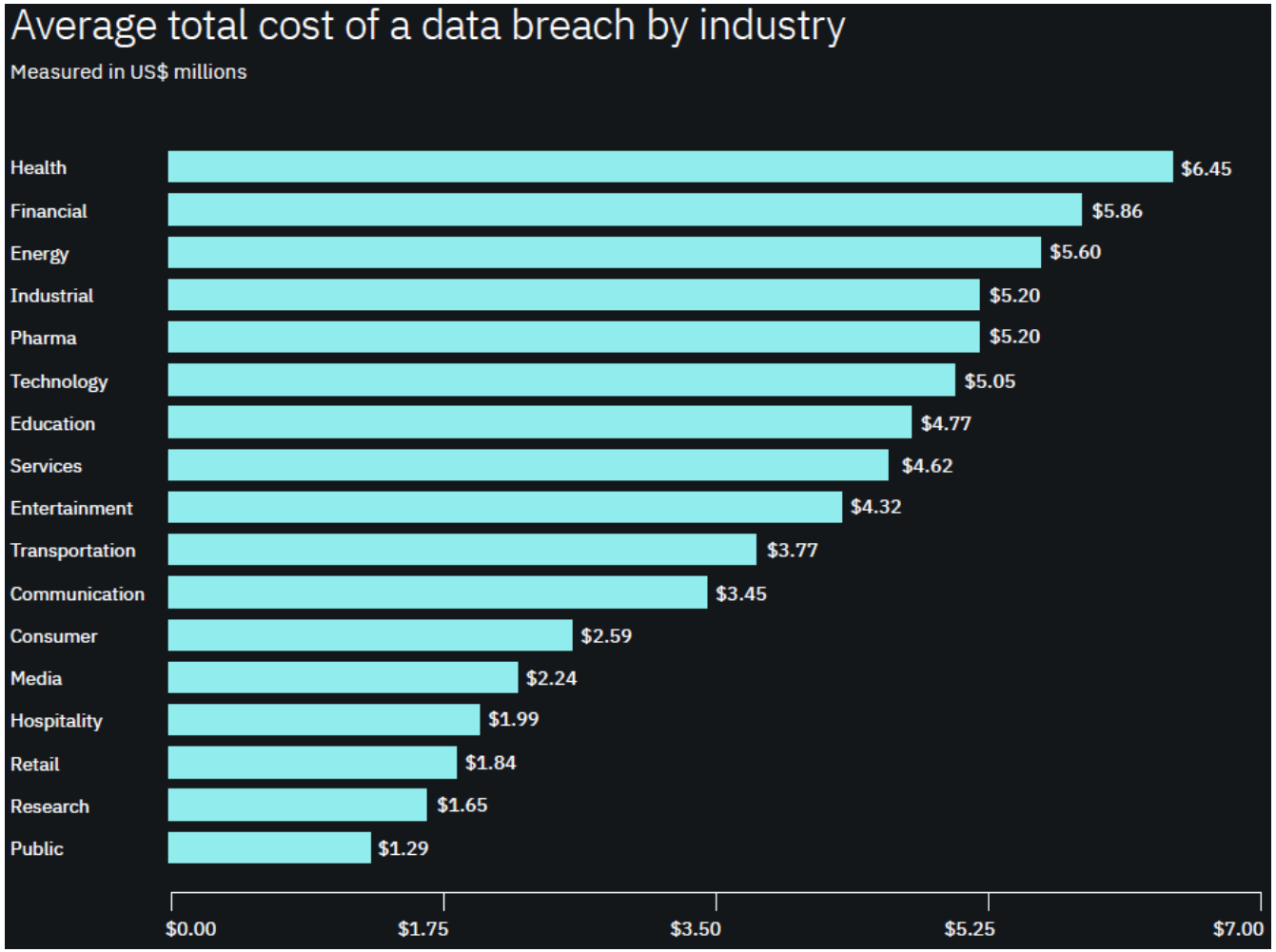
Covered entities are responsible for ensuring the issuance of:

- Reports to individuals whose PHI was subject to a breach in a timely manner, and at the least no more than 60 days after the discovery of the breach
- Reports to HHS within 60 days if the breach affected more than 500 individuals, or annually if the breach affected 500 or fewer individuals
- Reports to the media within 60 days of discovering a breach if a breach affected more than 500 individuals in any one state or jurisdiction

BAs must notify CEs of breaches (and fulfill any contractual obligations relating to the breach)

Why HIPAA Matters in Health Care Deals

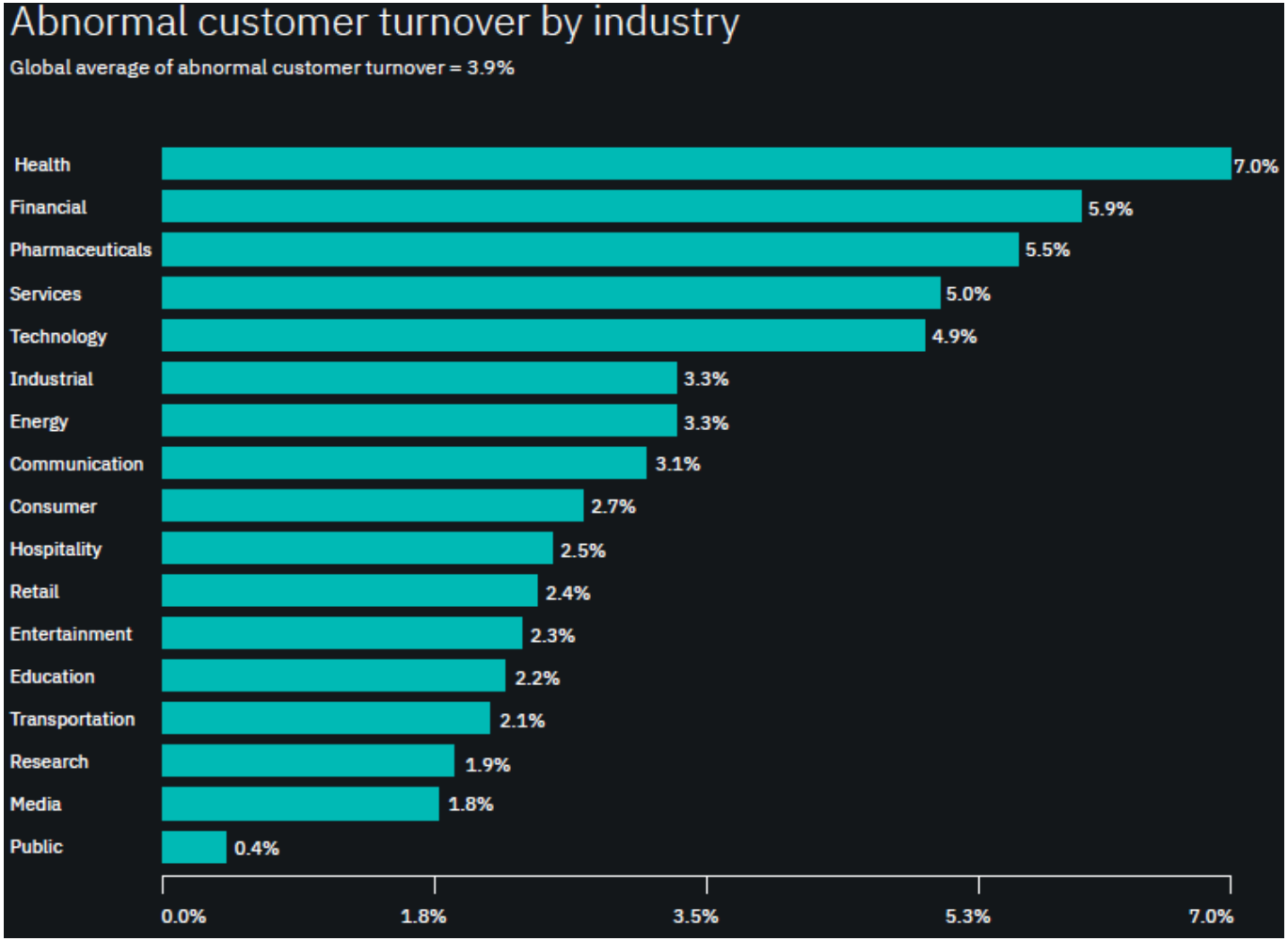
Data Breach Trends – Average Cost



The average total cost of a data breach in the health care industry was **$6.45** million, or **65** percent higher than the average total cost of a data breach.

Data from Ponemon Institute/IBM Security Cost of A Data Breach Report 2019

Data Breach Trends – Customer Turnover



Health care, financial services, and pharmaceutical companies have more trouble than other industries retaining customers after a breach.

Data from Ponemon Institute/IBM Security Cost of A Data Breach Report 2019

HIPAA Enforcement: July 2008 – May 2013

Date of Enforcement	Health Care Entity	Penalty or Settlement
July 2008	Providence Health & Services	Payment of $100,000 plus 3 year CAP
January 2009	CVS Pharmacy	Payment of $2,250,000 plus 3 year HHS CAP and 20 year FTC order
July 2010	Rite Aid	Settlement of $1,000,000 plus 2 year HHS CAP and 20 year FTC order
December 2010	Management Services Organization	Settlement of $35,000 plus 2 year CAP
February 2011	Cignet Health	Penalty of $4,300,000
February 2011	Massachusetts General Hospital	Settlement of $1,000,000 plus 3 year CAP
July 2011	UCLA Health System	Settlement of $865,500 plus 3 year CAP
March 2012	BCBST	Settlement of 1,500,000 plus 3 year CAP
April 2012	Phoenix Cardiac Surgery	Settlement of $100,000 plus 1 year CAP
June 2012	Alaska DHSS	Settlement of $1,700,000 plus 3 year CAP
September 2012	Massachusetts Eye and Ear	Settlement of $1,500,000 plus 3 year CAP
January 2013	Hospice of North Idaho	Settlement of $50,000 plus 2 year CAP
May 2013	Idaho State University	Settlement of $400,000 plus 2 year CAP

HIPAA Enforcement: June 2013 – November 2015

Date of Enforcement	Health Care Entity	Penalty or Settlement
June 2013	Shasta Regional Medical Center	Settlement of $275,000 plus 1 year CAP
July 2013	WellPoint	Settlement of $1,700,000
August 2013	Affinity Health Plan, Inc.	Settlement of $1,215,780 plus 120 day CAP
December 2013	Adult & Pediatric Dermatology, P.C.	Settlement of $150,000 plus 3 year CAP
March 2014	Skagit County	Settlement of $215,000 plus 3 year CAP
April 2014	Concentra Health Services	Settlement of $1,725,220 plus 2 year CAP
May 2014	New York and Presbyterian Hospital	Settlement of $3,300,000 plus 3 year CAP
June 2014	Parkview Health System, Inc.	Settlement of $800,000 plus 1 year CAP
December 2014	Anchorage Community Mental Health Services	Settlement of $150,000 plus 2 year CAP
April 2015	Cornell Prescription Pharmacy	Settlement of $125,000 plus 2 year CAP
June 2015	St. Elizabeth's Medical Center	Settlement of $218,400 plus 1 year CAP
September 2015	Cancer Care Group, P.C.	Settlement of $750,000 plus 3 year CAP
November 2015	Lahey Hospital and Medical Center	Settlement of $8500,000 plus 2 year CAP
November 2015	Triple-S Management Corporation	Settlement of $3,500,000 plus 3 year CAP

HIPAA Enforcement: December 2015 – October 2016

Date of Enforcement	Health Care Entity	Penalty or Settlement
December 2015	University of Washington Medicine	Settlement of $750,000 plus 2 year CAP
February 2016	Lincare, Inc.	Penalty of $239,800
February 2016	Complete P.T., Pool & Land Physical Therapy	Settlement of $25,000 plus 3 year CAP
March 2016	North Memorial Health Care	Settlement of $1,550,000 plus 2 year CAP
March 2016	Feinstein Institute for Medical Research	Settlement of $3,900,000 plus 3 year CAP
April 2016	New York Presbyterian	Settlement of $2,200,000 plus 2 year CAP
June 2016	Catholic Health Care Services of the Archdiocese of Philadelphia	Settlement of $650,000 plus 2 year CAP
June 2016	Oregon Health & Science University	Settlement of $2,700,000 plus 3 year CAP
July 2016	University of Mississippi Medical Center	Settlement of $2,750,000 plus 3 year CAP
August 2016	Advocate Health Care Network	Settlement of $5,550,000 plus 2 year CAP
September 2016	Care New England Health System	Settlement of $400,000 plus 2 year CAP
October 2016	St. Joseph Health	Settlement of $2,140,000 plus 3 year CAP

HIPAA Enforcement: November 2016 – February 2018

Date of Enforcement	Health Care Entity	Penalty or Settlement
November 2016	University of Massachusetts Amherst (UMass)	Settlement of $650,000 plus 2 year CAP
January 2017	Presence Health	Settlement of $475,000 plus 2 year CAP
January 2017	MAPFRE Life Insurance Company of Puerto Rico	Settlement of $2,204,182 plus 3 year CAP
February 2017	Children's Medical Center of Dallas	Penalty of 3,200,000
February 2017	Memorial Healthcare System	Settlement of $5,500,000 plus 3 year CAP
April 2017	Metro Community Provider Network	Settlement of $400,000 plus 3 year CAP
April 2017	Center for Children's Digestive Health	Settlement of $31,000 plus 2 year CAP
April 2017	CardioNet, Inc.	Settlement of $2,500,000 plus 2 year CAP
May 2017	Memorial Hermann Health System	Settlement of $2,400,000 plus 2 year CAP
May 2017	St. Luke's-Roosevelt Hospital Center	Settlement of $387,000 plus 3 year CAP
December 2017	21st Century Oncology, Inc.	Settlement of $2,300,000 plus 2 year CAP
February 2018	Fresenius Medical Care North America (FMCNA)	Settlement of $3,500,000 plus 2 year CAP
February 2018	Filefax, Inc.	Settlement of $100,000 plus indefinite CAP

HIPAA Enforcement: June 2018 – November 2019

Date of Enforcement	Health Care Entity	Penalty or Settlement
June 2018	University of Texas MD Anderson Cancer Center	Penalty of $4,348,000
September 2018	Boston Medical Center, Brigham and Women's Hospital, and Massachusetts General Hospital	Settlement of $999,000 plus 2 year CAP
October 2018	Anthem, Inc.	Settlement of $16,000,000 plus 2 year CAP
November 2018	Allergy Associates of Hartford, P.C.	Settlement of $125,000 plus 2 year CAP
December 2018	Advanced Care Hospitalists PL (ACH)	Settlement of $500,000 plus 2 year CAP
December 2018	Pagosa Springs Medical Center (PSMC)	Settlement of $111,400 plus 2 year CAP
February 2019	Cottage Health	Settlement of $3,000,000 plus 3 year CAP
May 2019	Touchstone Medical Imaging	Settlement of $3,000,000 plus 2 year CAP
May 2019	Medical Informatics Engineering, Inc. (MIE)	Settlement of $100,000 plus 2 year CAP
September 2019	Bayfront Health St. Petersburg	Settlement of $85,000 plus 1 year CAP
October 2019	Elite Dental Associates, Dallas	Settlement of $10,000 plus 2 year CAP
October 2019	Jackson Health System (JHS)	Penalty of $2,150,000
November 2019	The University of Rochester Medical Center	Settlement of $3,000,000 plus 2 year CAP

HIPAA Regulatory Challenges in Deals

Use or Disclose PHI for Health Care Operations

(a) ***Standard.*** A covered entity or business associate may not use or disclose protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) ***Covered entities:*** Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

45 C.F.R. § 164.502

Use or Disclosure for Health Care Operations

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

45 C.F.R. § 164.506

Health Care Operations

Health care operations means any of the following activities *of the covered entity* to the extent that the activities are related to covered functions:

(6) Business management and general administrative activities of the entity, including, but not limited to:

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity

45 C.F.R. § 164.501

Exception from the Sale of PHI

(a) ***Standard.*** A covered entity or business associate may not use or disclose protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(5) Prohibited uses and disclosures.

(ii) Sale of protected health information:

(B) For purposes of this paragraph, sale of protected health information means:

(2) Sale of protected health information does not include a disclosure of protected health information:

(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a); . . .

45 C.F.R. § 164.502(a)(5)(ii)(B)(2)

What Falls Safely Within This Framework?

- Deal between two covered entities
- Deal between a covered entity and a purchaser that will be a covered entity following closing
- Private equity?
- Business associates?
- Lawyers, accountants, advisors, funding sources?
- Multiple bidders?
- Transaction that does not close?

Minimum Necessary

(b) ***Standard: Minimum necessary***

(1) Minimum necessary applies**.** When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) ***Minimum necessary does not apply*****.** This requirement does not apply to:
(i) Disclosures to or requests by a health care provider for treatment;
(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;
(iii) Uses or disclosures made pursuant to an authorization under § 164.508;
(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;
(v) Uses or disclosures that are required by law, as described by § 164.512(a); and
(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

45 C.F.R. § 164.502(b)

Diligence

Diligence Goals

Fact Finding

- Questions to ask
- Documents to request

Inform Representations and Warranties in Transaction Agreement

- Key representations and warranties
- Draft representations to flush out diligence

Risk Allocation

- Indemnification
- Liability caps
- Breach costs
  - Breach investigation, mitigation, remediation costs
  - Notice costs; loss of goodwill
- Cyber insurance
- Equitable relief provisions

Post-Closing Planning

- Identify where buyer may need to allocate resources post-closing

HIPAA Diligence: Know Before You Buy

- **What is the HIPAA status of each entity involved in the transaction?**
- **Seller's HIPAA policies and procedures, past and present**
  - What HIPAA compliance procedures does the seller have in place?
  - How long have those policies and procedures been in place
  - Are they aspirational and forward-looking?
  - How much would it cost to implement adequate security and compliance procedures?
- **Have they experienced any incidents in the past that they elected not to report?'**
- **Who within each organization will have access to the data?**
  - Does everyone need to see the PHI?
- **What will happen to the PHI in case of a transaction that is not completed?**
- **What other state and federal privacy and data security laws might impact this transaction?**

HIPAA Status of the Parties

Is the target a covered entity?

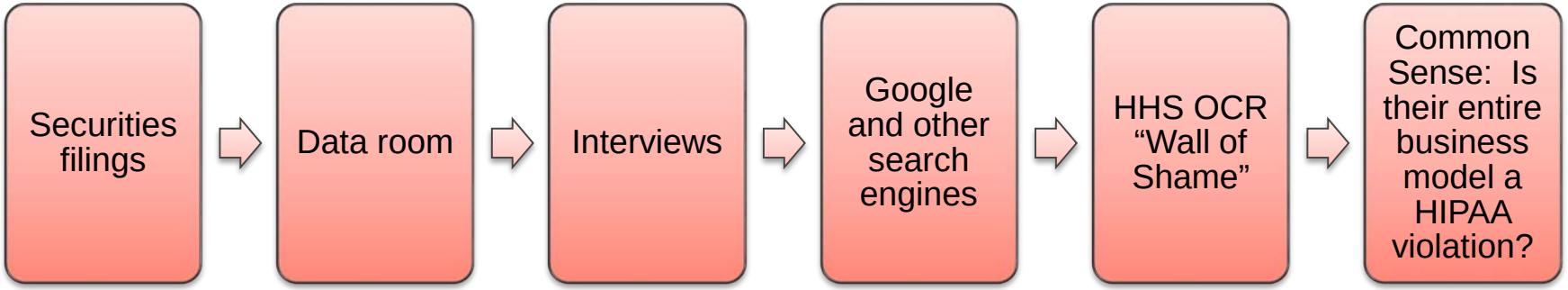
- Does the target engage in standard HIPAA transactions, and can it satisfy the definition of "health care provider"?

Is the target a business associate?

- Does the target *create, receive, maintain* or transmit PHI to perform a function or activity for or on behalf of a covered entity?
  - These functions and activities may include claims processing or administration, data processing, quality assurance, billing, benefit management, practice management, etc.
- Does the target provide professional services to a covered entity?
  - Professional services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services
  - Does the provision of those professional services involve the disclosure of PHI from or for the covered entity to your company?

Both business associates and covered entities have express flow-down obligations

Diligence Tools



Key Data Room Documents

- **When conducting HIPAA due diligence, consider requesting the following documents:**
  - HIPAA policies and procedures, including all breach notification procedures and data breach response plans
  - Documentation related to HIPAA training, including modules and training schedule
  - Internal and third-party HIPAA audits and records of subsequent corrective action, including any associated risk management plans
  - Current HIPAA Notice of Privacy Practices
  - Records of any OCR investigations and any other communications with an regulators (including state attorneys general) regarding potential HIPAA violations (related to a breach or otherwise)
  - All documentation related to significant internal or vendor data breaches, including records related to any breach reportable to any governmental authority, any data breach notices sent to individuals, and any breach notices from vendors
  - Any notices of threatened or pending lawsuits related to any data breach, HIPAA violation, or other applicable state or federal privacy or data security law
  - A list of all business associates
  - All contracts or services agreements with vendors that have access to PHI, including related BAAs
  - A copy of the target's standard form of BAA

Questions to Ask on the Diligence Call

Diligence calls provide an opportunity to ask clarifying questions and gather important context surrounding documents produced in the data room

For example, consider asking the following key questions:

- Can you describe your organization's management structure as related to HIPAA compliance? What types of issues are escalated to the top levels of that structure?
- Has the entity experienced any significant data breaches that are not reflected in data room documents? (Also, consider asking for more details related to breaches identified in the data room, as needed.)

Areas of Concern

Some of the main causes of a security breach are:

- Employee negligence
- External theft of a device
- Employee theft
- Phishing, including spear phishing
- Malware

Incident Response Plan

- Does the target have a written plan?
- Has it been tested/simulated?
- Are there protocols in the event of a breach to mitigate potential harm?

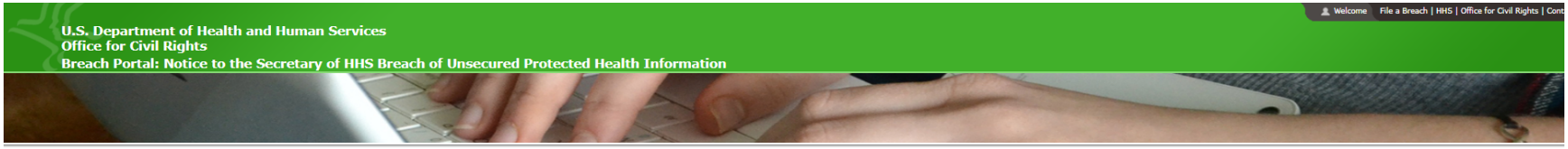
Training

- Phishing exercises work
- Privacy training
- Security training
- Should be on-going

Image source: https://themerkle.com/beware-coinbase-phishing-scam/

Practice Tip: Asking the right questions will enable a buyer to craft tailored representations that hold a target accountable for responses provided through diligence.

HHS OCR "Wall of Shame"



Under Investigation | Archive | Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Utah Valley Eye Center	UT	Healthcare Provider	20418	11/01/2019	Hacking/IT Incident	Desktop Computer
	Prisma Health - Midlands	SC	Healthcare Provider	19060	10/28/2019	Hacking/IT Incident	Other
	Virginia Department of Behavioral Health & Developmental Services	VA	Healthcare Provider	1442	10/25/2019	Unauthorized Access/Disclosure	Network Server
	The Kroger Co., for itself and its affiliates and subsidiaries	OH	Healthcare Provider	4812	10/25/2019	Loss	Paper/Films
	The Kroger Co., for itself and its affiliates and subsidiaries	OH	Healthcare Provider	2752	10/25/2019	Loss	Paper/Films
	TOTS & TEENS PEDIATRICS	TX	Healthcare Provider	31787	10/24/2019	Hacking/IT Incident	Network Server
	The Affiliated Sante Group	MD	Healthcare Provider	679	10/24/2019	Theft	Laptop
	Wheatland Dental Care	IL	Healthcare Provider	955	10/24/2019	Hacking/IT Incident	Other
	Greater Cincinnati Pathologists, Inc.	OH	Healthcare Provider	7725	10/23/2019	Hacking/IT Incident	Email
	Texas Health Harris Methodist Hospital Hurst-Euless-Bedford	TX	Healthcare Provider	4804	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Presbyterian Hospital Dallas	TX	Healthcare Provider	12415	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Hospital Alliance	TX	Healthcare Provider	3784	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Presbyterian Hospital Denton	TX	Healthcare Provider	6688	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Hospital Azle	TX	Healthcare Provider	2113	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Hospital Cleburne	TX	Healthcare Provider	2737	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Hospital Southwest Fort Worth	TX	Healthcare Provider	7478	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Presbyterian Hospital Rockwall	TX	Healthcare Provider	4789	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Hospital Stephenville	TX	Healthcare Provider	1348	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Harris Methodist Southlake	TX	Healthcare Provider	525	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Arlington Memorial	TX	Healthcare Provider	6187	10/22/2019	Unauthorized Access/Disclosure	Other
	Texas Health Presbyterian Hospital Plano	TX	Healthcare Provider	9678	10/22/2019	Unauthorized Access/Disclosure	Other

HHS OCR "Wall of Shame"– Advanced Search

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Hide Advanced Options

Breach Submission Date: From: To:

Type of Breach:
- ☐ Hacking/IT Incident
- ☐ Improper Disposal
- ☐ Loss
- ☐ Theft
- ☐ Unauthorized Access/Disclosure
- ☐ Unknown
- ☐ Other

Location of Breach:
- ☐ Desktop Computer
- ☐ Electronic Medical Record
- ☐ Email
- ☐ Laptop
- ☐ Network Server
- ☐ Other Portable Electronic Device
- ☐ Paper/Films
- ☐ Other

Type of Covered Entity: -- Choose Covered Entity Type --

State: -- Choose State --

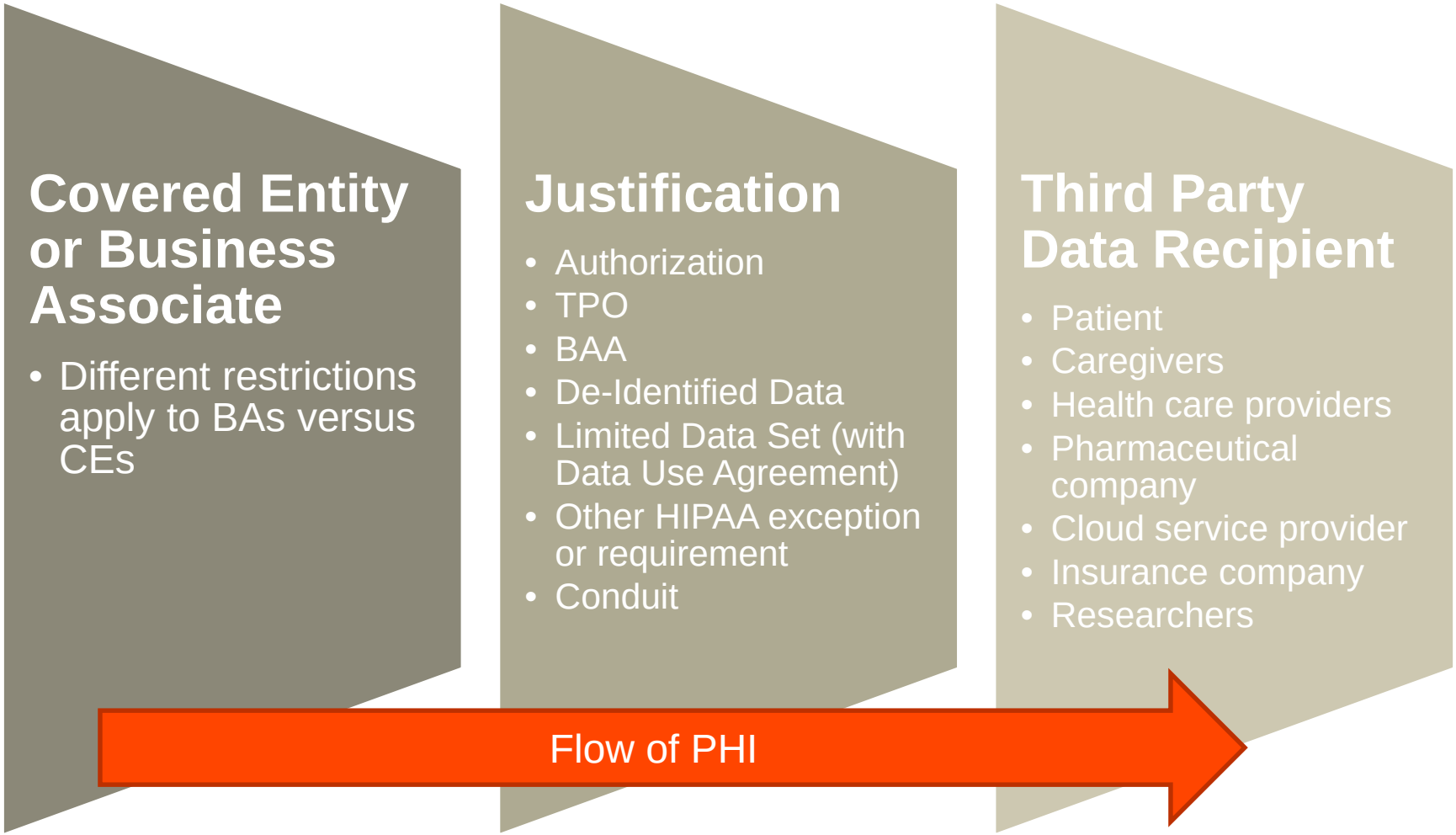
Business Associate Present?: --

Description Search:

CE / BA Name Search:

Apply Filters

HIPAA-Legitimacy of Target's Business Model



“De-Identified” Data?

De-identified data is not PHI and is not subject to HIPAA

- HIPAA “de-identified” information is health information that has been stripped of all identifiers and cannot reasonably be used to identify an individual
- Two methods of de-identification under HIPAA

Statistical Method

- Certification by a qualified statistician

Safe Harbor Method

- Removal of 18 enumerated identifiers and ensuring that the remaining information could not be used alone or in conjunction with other information to identify the individual
- 18 identifiers that must be removed include:
  - Names
  - Dates (except year) relating to the patient
  - Zip codes, city
  - IP Addresses and Web URLs
  - Full face photographs
  - Biometric identifiers

Deal Documents

Overview

- Restructuring Agreement
- Separation Agreement
- Purchase Agreement
- Transition Services Agreement
  - Business Associate Agreement – reciprocal?
  - Privacy and Information Security Agreement – reciprocal?
- Loan Agreement
- Disclosure Schedules

Definitions

Ensure the data and data law vocabulary is sufficiently robust to allow for appropriate differentiation

- Sensitive Data
- Personally Identifiable Information or Personal Data
- Protected Health Information
- De-Identified Data
- Proprietary Information
- Business Information
- Confidential Information
- Data Breach
- Security Incident
- HIPAA
- Data Protection Law
- Health Care Laws
- Law

Think Beyond PHI

Define "Personal Data" broadly to include any and all information that could be used to identify an individual, with a specific focus on information protected by law

- "Personal Data" means any individually identifiable information (or information that, in combination with other information, could allow the identification of an individual), including demographic, health, behavioral, biometric, financial, nonpublic and geolocation information, IP addresses, network and hardware identifiers, employee information and any other information that is protected under any applicable privacy, data security, or data breach notification law (including HIPAA, the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) ("GLBA"), and PCI-DSS), or which the target is required to safeguard under any of its contractual obligations

Define "Sensitive Data" to include both Personal Data and sensitive business data

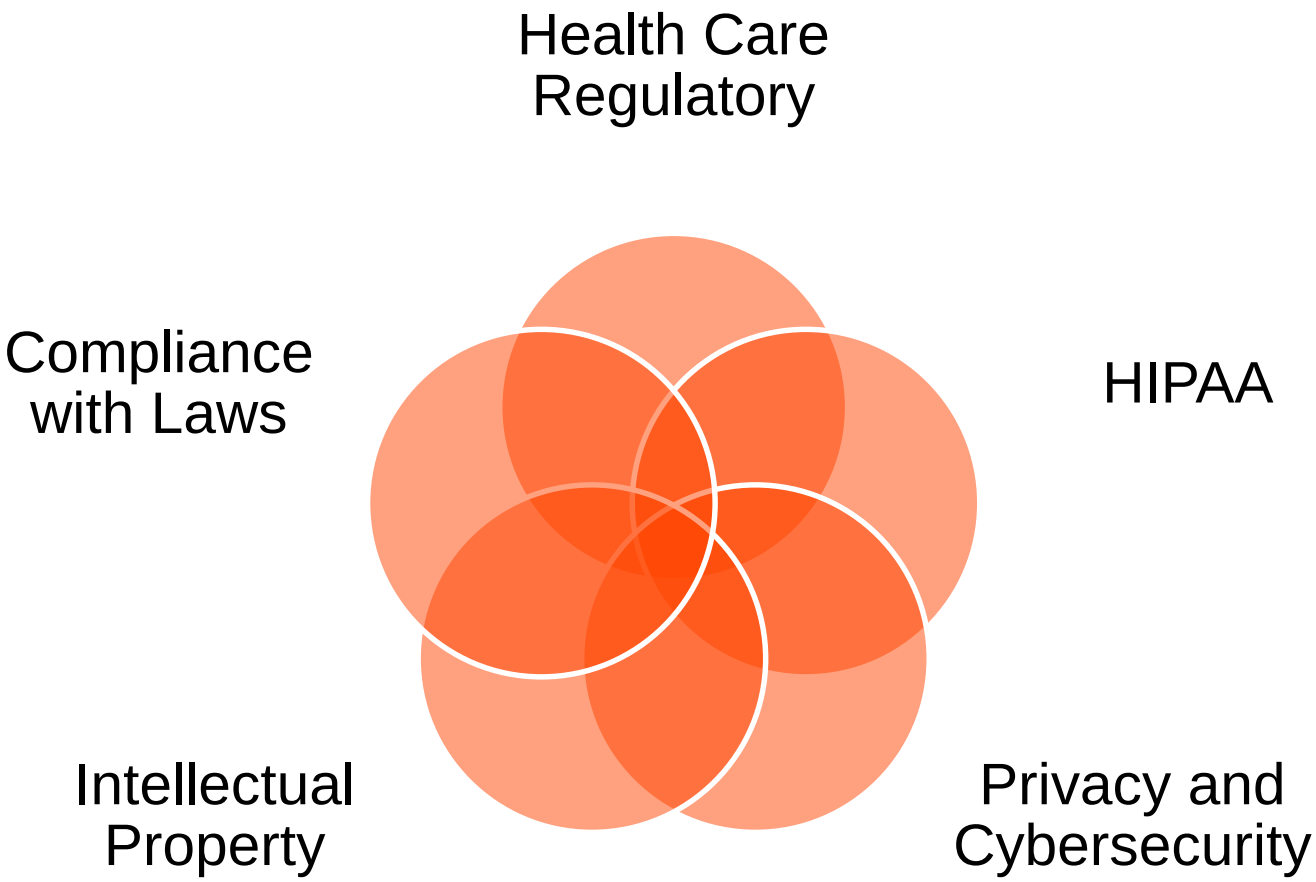
- "Sensitive Data" means all Personal Data, confidential information, proprietary information, trade secrets, intellectual property and any other information protected by applicable law or contract that is collected, maintained, stored, transmitted, used, disclosed or otherwise processed by, for or on behalf of the target or any of its subsidiaries

Why both Personal Data and Sensitive Data?

- Most legal frameworks protect Personal Data, while sensitive business information (also vulnerable to hackers and data breaches) should also be addressed under some representations

Practice Tip: Every company has individually identifiable information protected by law related to its employees (not just patients).
Example: Breach notices sent to terminated employees explaining that their dependents' SSNs were disclosed by a negligent benefits vendor can lead to lawsuits.

Where will the HIPAA terms sit?



Seller Representations: Risk Shifting

- Adequacy and fitness of administrative, technical and physical safeguards to protect data and the target's IT systems
- Compliance with privacy law (domestic and foreign, including HIPAA)
- Compliance with internal and external privacy policies (including HIPAA policies and procedures)
- Compliance with contractual obligations on protection, use, and disclosure of data
- Periodic cybersecurity audits and risk assessments
  - Remediation of any identified deficiencies and weaknesses
- Routine review and testing of the target's breach response and disaster recovery plans, procedures, and policies

Seller Representations: Use Schedules to Flush Out Diligence

- **Data Breaches**. Schedule any material privacy or data security breaches, including unauthorized access, acquisition, exfiltration, manipulation, erasure, use, or disclosure of PHI or other classes of data
- **Business Associate Breaches**. Schedule any known service provider or vendor breaches
  - Schedule any material failures, or presence of malware, viruses, ransomware, bugs, or other malicious code in the target's IT systems that have caused material disruptions or interruptions in or to the use of the target's IT systems
  - Schedule any required notifications made pursuant to any breach notification law or contract provision

Practice Tip: Business associates may have access to significant data assets, and are often an entity's weakest link. Look for:

- Evidence of vendor cybersecurity diligence (pre-engagement)
- Evidence of ongoing vendor monitoring (post-engagement)
- Contractually shifting notice obligations in the event of a breach from the target to the vendor

Materiality Qualifiers

When is a materiality qualifier appropriate?

- Buyer wants clean representations, seller wants qualified representations
- Every company has data incidents in the ordinary course of business – you can use materiality in conjunction with schedules to identify significant breaches or other security incidents

Use of a materiality qualifier is tied to deal leverage and risk tolerance

Which representations do we see with a materiality qualifier most often?

- Target breaches
- Target system failures
- Vendor breaches
- Compliance with law, policies and contractual obligations
- Remediation of weaknesses identified in security audits

Materiality Waterfall

- Material
- Material to the Company and its subsidiaries taken as a whole: A high standard, but reasonable in some circumstances
- Material Adverse Effect: An extremely high bar, rarely met in practice (and largely negating protection under the representation)

Knowledge Qualifiers

Knowledge qualifiers can be more restrictive than materiality qualifiers

- Actual knowledge vs. constructive knowledge (i.e., should have known)
- Due inquiry
- Reasonable diligence

When is a knowledge qualifier potentially appropriate?

- Vendor breaches
- Allocating risk of undiscovered breaches between buyer and seller
- Compliance with contractual obligations

As with materiality, use of a knowledge qualifier is tied to deal leverage and risk tolerance

Practice Tip: Whom to include within the knowledge group

Standard Practice: CEO, CFO, VPs are standard in M&A deals, but material, non-catastrophic breaches may not reach these officers.

Best Practice: Be sure to include the Chief Information Security Officer, Chief Privacy Officer or similar position. Use due diligence to identify the target's reporting structure and the person in the best position to have knowledge of material cybersecurity issues.

Look-Back Periods

Look-backs function as qualifiers and can have a major impact on liability

- Are in compliance with HIPAA
- For the past 3 years – or 6 years – have been in compliance with HIPAA

Factors to consider in determining when a look-back may be appropriate

- Breaches
- Compliance with law
- Compliance with policies and procedures
- Major changes in target management

TSA – Ask the Right Questions Regarding Privacy and Cybersecurity

- What data will this party collect, create, use, disclose, maintain, transmit, store, destroy, or otherwise access or process, and for what purpose, as part of this relationship?
- What privacy and security standards will apply?
- What would happen if there is a data breach? How would roles and responsibilities be allocated between the parties? What else could go wrong?
- How does the contract address liability – through indemnity, liability caps, and insurance requirements?
- Must the vendor train its workforce or maintain written privacy and data security policies and procedures?
- What rights do the parties have to use and disclose data that is collected through the relationship?
- What rights, obligations, and needs do the parties have with respect to data upon termination?
- Under what circumstances – relevant to privacy or cybersecurity – would you want to be able to terminate the vendor agreement?

Treat the other party to the TSA like any other vendor, unless the TSA is reciprocal

TSA – Core Privacy and Security Terms

Consider whether a BAA or PISA is needed

Information Use and Disclosure

- Be clear about the nature and scope of information that will be shared with the vendor, where relevant
- Affirmatively permit the vendor to use and disclose data, as appropriate
- Restrict the use and disclosure of data for purposes that are not reasonably necessary for vendor services, or that are not permitted or required by law
- Address whether the vendor is prohibited from identifying data or from contacting individuals who are data subjects, and whether the vendor may de-identify data, as appropriate

Information Security

- Contractually obligate the vendor to implement and maintain reasonable and appropriate administrative, technical and physical safeguards to protect your company's sensitive data
- Require security audits, including remediation
- Hold the contractor to more granular requirements, as appropriate

TSA – Risk Allocation

Indemnity

- Obtain appropriate indemnification for claims relating to data breaches or other privacy or cybersecurity violations
  - Actor (affiliates, employees, contractors, workforce)
  - Threshold (acts and omissions, negligence, gross negligence, fraud and intentional misconduct)
  - Proximity (arising from, relating to)
  - Indemnified and indemnifying party
  - Scope (third party claims, fines, penalties, settlements, class action suits)
- **Remember: Reciprocal does not necessarily equate to fair**

Costs

- Breach investigation and mitigation (including forensics, breach containment, etc.)
- Breach response (including notices to individuals and other third parties)
- Breach remediation (identity monitoring, identity theft insurance, etc.)

Practice Tip: Be prepared to fight the good fight on indemnity!

TSA – Risk Allocation

Liability Cap

- Is the liability cap reasonable?
- Are carve-outs from liability caps needed?

Warranties

- Review the warranties critically: Are the disclaimers inappropriate given HIPAA and other cybersecurity risks? Does the vendor specifically disclaim liability for data loss, security breach, etc.?

Insurance

- Require the vendor to maintain appropriate levels of cyber insurance, given the risks

Responsibility for Compliance

- Which party is responsible for determining whether a requested data use, disclosure, or control is permissible under applicable law?

Equitable Relief

TSA BAA: Mandated Contract Terms – Privacy Rule

Under the HIPAA Privacy Rule, a BAA must, at a minimum, provide that a business associate will:

- Establish the permitted and required uses and disclosures of PHI, and may not authorize the business associate to use or further disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity
- Not use or further disclosure of PHI except as permitted by the contract or required by law
- Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the BAA
- Report to the covered entity any use or disclosure of PHI not provided for in the BAA, including breaches of unsecured PHI
- Ensure all subcontractors are bound by the same restrictions and conditions
- Comply with individual rights obligations (relating to the individual's ability to access and amend PHI, and to receive an accounting of disclosures)
- If carrying out a covered entity obligation under the Privacy Rule, comply with the relevant Privacy Rule requirements
- Make its internal books and records available to the Secretary to determine the covered entity's compliance with HIPAA
- If feasible, return or destroy all PHI upon termination of the contract

The upstream entity must also be able to terminate the contract if it determines the business associate violated a material term

TSA BAA: Mandated Contract Terms – Security Rule

Under the HIPAA Security Rule, a BAA must provide that a business associate will:

- Comply with all applicable requirements of the Security Rule
  - Ensure the confidentiality, integrity, and availability of ePHI
  - Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI
  - Protect against reasonably anticipated but not permitted uses or disclosures of ePHI
  - Adopt Administrative Safeguards
  - Adopt Physical Safeguards
  - Adopt Technical Safeguards
  - Implement reasonable and appropriate policies and procedures to comply with the Security Rule
- Ensure that any subcontractors that create, receive, maintain or transmit ePHI comply with the requirements of the Security Rule
- Report to the covered entity any security incident of which it becomes aware (including breaches of unsecured PHI)

TSA BAA: Mandated Contract Terms – Breach Notification

Under the HIPAA Breach Notification Rule, a BAA must provide that a business associate will:

- Notify the covered entity of a breach of unsecured PHI
  - Timeliness
  - Breaches treated as discovered
  - Content of the notification

TSA – Incident Reporting and Response, Beyond HIPAA

Incidents Triggering Reporting

- Security incident affecting any sensitive data
- Breach of unsecured personal data
- Use or disclosure of sensitive data not permitted by contract

Report Timeframes and Content

Incident Response Roles and Responsibilities

- Require that the vendor investigate and promptly report to you any actual or suspected unauthorized uses or disclosures of your sensitive data
- Protect your good name (and goodwill) by obligating the vendor to provide any required notice to individuals and the government—on vendor letterhead—of any breach

What's the Risk?

Privacy and Cybersecurity Risks in Business Deals

Regulatory Compliance Risks

- Sensitive personally identifiable information is often protected by law, enforced by regulators such as HHS OCR, Attorneys General, and the FTC

Litigation Risks

- Failure to provide the level of security promised in online privacy policies, required by law, or obligated by contract may create litigation risks
  - Breach of contract
  - Class action lawsuits

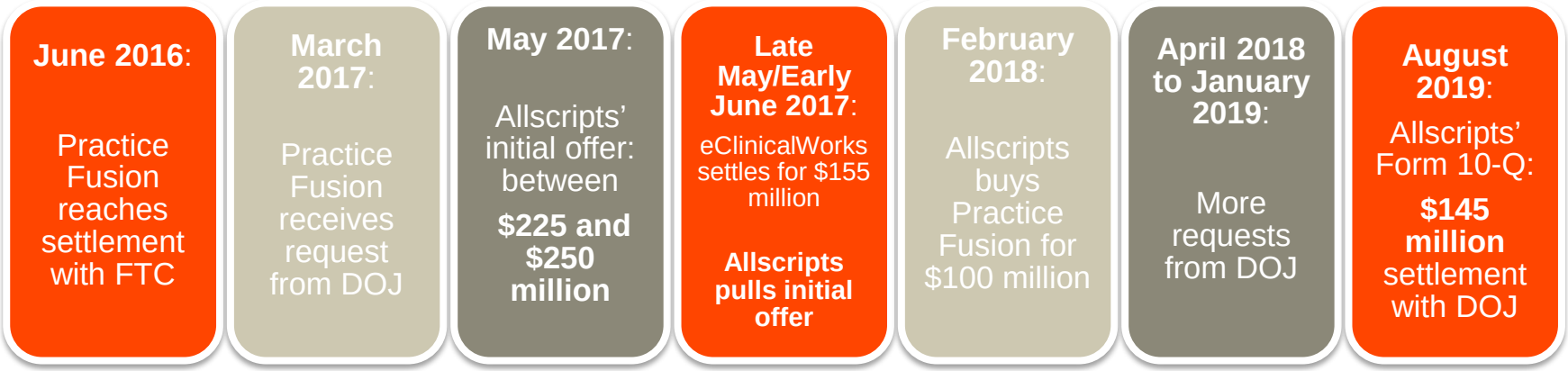
Business Continuity

- Failure to secure the target's IT infrastructure and have appropriate disaster recovery plans puts the day-to-day operations of the business at risk

Goodwill

- One of the most significant costs of a material data security incident is the loss of goodwill—and patients or other customers—from a publicly disclosed breach

Case Study: Allscripts and Practice Fusion



What Can You Be Sued For?

- Breach of state law notification requirements – you failed to properly notify me
- Negligence – you did not exercise reasonable care in protecting my data
- Negligent misrepresentation – you told me you would protect my data
- Breach of contract – you pledged to protect my data and failed to do so
- Conversion – I lost ownership of my data because you failed to protect it
- Unjust enrichment – I paid you in part to protect my data
- Breach of fiduciary duty – I entrusted my data to you
- Invasion of privacy – you violated my reasonable expectation of privacy
- Identity theft – you allowed my identity to be stolen
- Damages – you are going to pay for this
- Injunction – I have to stop you from using my data
- Regulatory enforcement from various agencies

Closing Thoughts

Speaker

Jo-Ellyn Sakowitz Klein, J.D., CIPP/US. For almost 20 years, Jo-Ellyn Sakowitz Klein has focused on privacy and data security matters for clients. She handles privacy, data security, data breach preparedness and data breach response matters for clients across many industries, with a special emphasis on the health sector. Jo-Ellyn was recognized in *The Legal 500 US* for Cyber law (including data privacy and data protection) in 2019.