EPSTEIN BECKER GREEN

How to Cut Down on Security Risks: What You Don't Know About HIPAA Security

October 29, 2015

Presented by

Adam Solander

Member of the Firm

asolander@ebglaw.com

202.861.1884

Agenda

1. Overview and State of Health Care Security
2. Auditing and Monitoring
3. Amendments and Corrective Action
4. Education and Training (Directors, Officers, Managers and All Employees)
5. Interface of legal requirements with practical considerations

EPSTEIN BECKER GREEN

Overview

The New Reality: Health and Device Industries Under Attack

"The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data."

- FBI Flash Alert, Aug., 2014

EPSTEIN BECKER GREEN

State of Health Care Industry

- **Unprepared and Under Attack**
  - The Law: HIPAA is an unarticulated standard. There are only a few required implementation specifications.
    - For example: Encryption is only addressable
  - Most of the security articulation comes from the required implementation specification requiring a Risk Assessment.
    - Organizations must, "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the security, confidentiality, integrity, and availability of electronic protected health information held by its self and its business partners."
    - Then Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
  - Given the squishiness of the HIPAA standard the maturity of information security programs varies greatly.

EPSTEIN BECKER GREEN

State of Health Care Industry

- The Verizon Breach Report identifies how breaches occur across selected industries.
- It is my opinion that the breaches in health care are low because we are not sophisticated enough to detect them. We basically report lost devices.

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

EPSTEIN BECKER GREEN

State of Health Care Industry

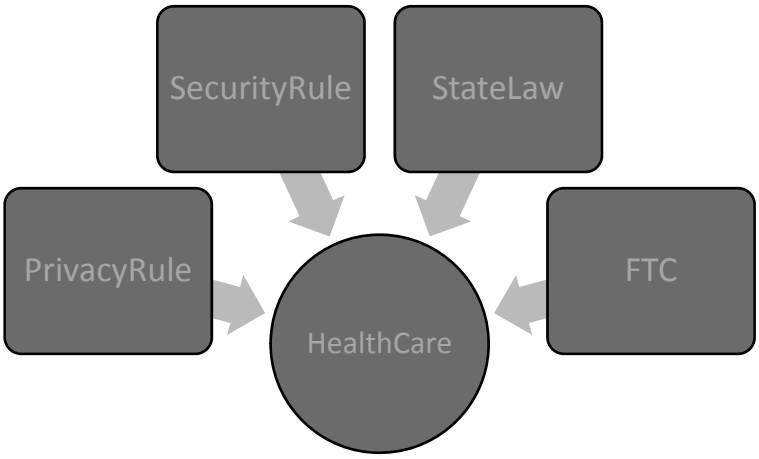
- Security is relatively new for a lot of health care companies. We are all scrambling to protect ourselves.
  - Shock wave: Late 2014 Community Health Systems was the first real hack followed quickly by Anthem in early 2015. FBI issues their flash warning in August immediately following the CHS breach.
  - Now every board in America is asking what can we do to prevent this from happening to us.
- Health Care Companies are designed to be open and share information quickly, systems not designed with security in mind.
  - Unpatchable systems common
  - Physical access easy
  - Lots of paper
- Health Care accounts for 17% of GDP, so anything not bolted down is being bought up which leads to huge integration issues and inconsistent security across an organization.
- Health care companies lack the IS resources, program maturity, and processes. We see paper programs with no operational effectiveness.

EPSTEIN BECKER GREEN

EPSTEIN BECKER GREEN

Legal and Enforcement Overview

Overview



EPSTEIN BECKER GREEN

Overview
Legal

HIPAA Privacy Rule:
The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other protected health information. The Rule requires appropriate safeguards to protect the privacy of protected health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

HIPAA Security Rule:
The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

State Law:
Forty-seven states have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, medical information etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

FTC:
The Federal Trade Commission has the authority under Section 5 of the FTC Act to enforce against entities engaged in unfair or deceptive practices. Recently, the FTC has used this authority to bring enforcement actions against entities who violate consumer privacy rights or fail to maintain appropriate security for private consumer information, including health care entities. The FTC also enforces against entities who do not obey their own stated privacy or security policies.

EPSTEIN BECKER GREEN

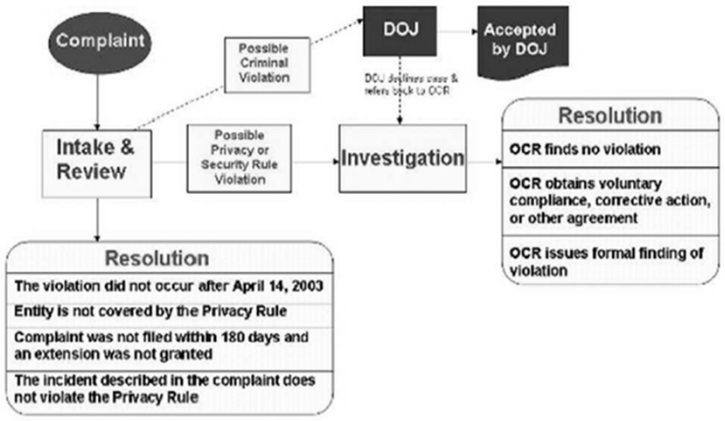
HIPAA
Compliance

". . . [Y]ou do have to have assertive enforcement; you have to have credible enforcement, that really does play a critical role in obtaining compliance . . . ."

-Leon Rodriguez

EPSTEIN BECKER GREEN

HIPAA
Compliance Process



EPSTEIN BECKER GREEN

Reported Breaches
Investigation Criteria

- OCR investigates ALL breaches involving over 500 individuals
  - Need to report within 60 days of discovery
  - Stay off the OCR wall of shame
- OCR investigates high profile breaches
  - Breach reports of less than 500 sent to Regional HHS office
    - Need to report < 500 breaches at end of year
  - Regional office has discretion to pursue
  - OCR enforced against Hospice of North Idaho
  - Stay out of the media

EPSTEIN BECKER GREEN

Civil Monetary Penalties ("CMP")
Framework

Standard of Culpability	Penalty/violation	Maximum Penalty
Did not know and by exercising reasonable diligence would not have known of violation	Corrective action without penalty	No penalty--however, subject to discretion of Secretary
Unknowing Violations	$100 - $50,000	$1,500,000
Violation due to reasonable cause	$1000 - $50,000	$1,500,000
Violation due to willful neglect	$10,000 - $50,000	$1,500,000
Willful neglect and violation not corrected within 30 days CE knew or should have known	$50,000	$1,500,000

Determining CMP
Important Factors

- Nature of the violation
- Circumstances, including the consequences of the violation
- Degree of culpability
- History of prior compliance
- Financial condition of the covered entity
- Such other matters as justice may require

Recent Enforcements
Cancer Care Group

- On September 2, 2015 OCR announced a settlement with CCG stemming from an August 29, 2012 incident involving the theft of an unencrypted laptop and storage device containing 55,000 patients' information
- OCR identified two main differences:
  - No risk assessment
  - No policy on portable media
- CCG paid $750,000 and agreed to a corrective action plan

EPSTEIN BECKER GREEN

State AG Enforcement
Example

- Triple-S Management Corp, Puerto Rico - $6.8 M
  - In September 2013, subsidiary accidentally mailed to approximately 70,000 Medicare Advantage beneficiaries a pamphlet that inadvertently displayed Medicare Health Insurance Claim Numbers ("HICNs"), which are considered protected health information under HIPAA
  - Additionally, the Puerto Rico Health Insurance Administration imposed administrative sanctions, including the suspension of all new enrollments, new dual eligibles and the obligation to notify affected individuals of their right to disenroll.

EPSTEIN BECKER GREEN

EPSTEIN BECKER GREEN

Auditing and Monitoring: Conducting the Risk Assessment

What is a Risk Assessment

The Risk Assessment is the foundational step in any security management process.

- Requires regulated entities to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of sensitive information held by the entity.
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Risk Assessments can be conducted using many different methodologies.

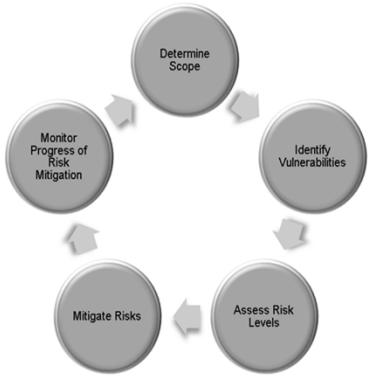
- What is appropriate depends of the organization (HIMSS, NIST, Custom)
- What you put in is what you get out
- Physical, Technical, and Administrative

EPSTEIN BECKER GREEN

Risk Assessment Process

NIST 800-30

1. Scope the Assessment
2. Gather Information
3. Identify Realistic Threats
4. Identify Potential Vulnerabilities
5. Assess Current Security Controls
6. Determine Likelihood and Impact of Threat
7. Determine the Level of Risk
8. Recommend Security Controls
9. Document Results



EPSTEIN BECKER GREEN

Risk Assessment Process

Scoping the Assessment

- Identify <u>where</u> sensitive information is created, received, maintained, processed and transmitted
  - Physical boundaries, technical environment, end user machines, paper storage, etc…
- Goal: Understand where sensitive information and systems reside

Gather Information

- Identify <u>how</u> sensitive information is created, received, maintained and processed
  - Determine security controls in place to protect
- Goal: Find hidden repositories of sensitive information or business process outside of secure environment

EPSTEIN BECKER GREEN

Risk Assessment Process

Identify Realistic Threats

- Identify potential threat sources to your sensitive information or systems
  - Ex., Social engineering attacks on the rise in my industry
  - Don't forget about physical and environmental

Identify Potential Vulnerabilities Based on Threats

- After identifying threats, document vulnerabilities that could be exploited by the threats
  - Ex., Employees have not been trained on social engineering

Assess Current Security Controls

- Based on the threats and vulnerabilities, determine whether current security controls are adequate to protect sensitive information
  - Technical testing needed

EPSTEIN BECKER GREEN

Risk Assessment Process

Determine Likelihood and Impact of a Threat Exercising a Vulnerability

- Prioritize the impact levels associated with a compromise based on a qualitative and quantitative assessment of the sensitivity and criticality of those assets
  - Confidentiality, Integrity, Availability
  - For example, could be harmed because of a loss of availability? Are denial of service attacks common?

Determine Risk

- Operationalizes previous step by analyzing the likelihood of a threat occurrence and the resulting impact
  - If someone could be harmed because of a loss of availability, and denial of service attacks are common, then High threat likelihood and High impact

EPSTEIN BECKER GREEN

Risk Assessment Process

Recommend Security Controls

- Based on the risk to the organization, recommend controls to reduce the level of risk to the IT systems and data to an acceptable level
- It is not possible to implement all recommended security controls. Use a cost benefit analysis to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk

Document and Mitigate

- Cyclical- process of mitigating and testing
- Topic of Next Crash Course

Practical Considerations

Identify Realistic Threats and Vulnerabilities

- Not an exercise in one's imagination
- Be careful of vendor chosen- get samples of product, mitigation plans

Don't Create "Bad Paper"

- Attorney-Client Privilege
- Legal: applying fact to law

Not a Paper Process

- To understand technical risk, vulnerability and likely penetration testing needed

Perform on a Regular Basis

- Choose your interval and document in policy
- Perform anytime change in environment: acquisitions, new infrastructure, new business partner

EPSTEIN BECKER GREEN

Amendments and Corrective Action: How to Implement a Corrective Action Plan

Introduction

- After conducting a risk assessment, an organization must respond to identified risks and reduce risk to an acceptable level
  - Maintain the confidentiality of data
  - Assure the integrity and availability of data
- Four basic approaches to risk control
  - Accept
  - Avoid
  - Transfer or share
  - Mitigate
- Need entire organization on board

Risk Acceptance

- Acknowledging a risk and making a conscious decision to accept the consequences
  - Risk is within the organization's risk tolerance
  - Not cost-effective to address
- Before accepting a risk, an organization should conduct a documented analysis that includes:
  - Likelihood of risk
  - Potential loss from risk
  - Cost of controls
  - Decision to accept the risk
- Regularly review risk acceptance decisions

Risk Avoidance

- Taking action to try to eliminate the risk
  - Source of risk
  - Exposure to the risk
- May be appropriate when the risk exceeds the organization's risk tolerance
- Often expensive
  - Consider opportunity cost

Risk Transfer

- Shifting responsibility for a risk to another party
  - Normally through cyber insurance
  - Indemnification
  - Outsource
- May be an attractive option when it's difficult to reduce the risk to an acceptable level
- Generally doesn't reduce likelihood of risk
- Secondary effects
  - Negative publicity
  - Dependency/loss of control

EPSTEIN BECKER GREEN

Risk Mitigation

- Taking action to reduce the probability and/or potential loss associated with a risk
- Involves implementing controls
  - Preventive vs. detective
- Cost-benefit analysis
  - Cost of control vs. projected benefits
  - If benefits > cost of control: consider implementing control
  - If cost of control > benefits: explore other controls or accept/avoid/transfer the risk

EPSTEIN BECKER GREEN

Considerations

- Develop an overall risk response strategy
  - Establish organizational risk tolerance
  - Outline goals and objectives
  - Provides the basis for determining whether to accept, avoid, transfer, or mitigate risk
- Prioritize
- Consider interim measures
- Detailed documentation
  - Mitigation strategies
  - Analyses and decisions

EPSTEIN BECKER GREEN

Risk Monitoring

- Risk management is an ongoing process
- Continue to monitor risk responses with respect to:
  - Compliance
    - Organizational mandates
    - Federal/state mandates
  - Effectiveness
    - Have the measures been effective in reducing risk to an acceptable level?
  - Changes
    - Systems
    - Environments

EPSTEIN BECKER GREEN

EPSTEIN BECKER GREEN

Training

HIPAA Training

- "[T]rain all members of its workforce on the policies and procedures with respect to protected health information…, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity"
  - To each member of the covered entity's workforce by no later than the compliance date for the covered entity
  - Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
  - To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures…, within a reasonable period of time after the material change becomes effective
- The days of generic training should be over…

EPSTEIN BECKER GREEN

Practical Consideration
Training and Risk Mitigation

- Many of the most damaging breaches have resulted from social engineering or employees with their own processes or data repositories
  - Organizations must assess whether their current training protects organization
  - Identify employees with processes outside of workflow

Practice Tips

- Understand what company information is available to con artists (social media, org charts etc.)
- Develop protocol for transmitting sensitive data or system credentials (e.g. IT will never ask for this information)
- Train on identification of fraudulent communications
- Interview employees to determine whether secondary processes have been created
  - Ex., transmission, storage, and device

Practical Consideration
Training on Paper

- Health care is still dependent on paper
- Well publicized well documented breaches are not a great target for ID theft
- Must train employees on proper handling of paper
  - Storage
  - Disposal
  - Creation

Practical Consideration
Culture of Compliance

- If you see something… say something!
  - Consider an anonymous protocol for reporting violations
  - Consider an FAQ document of common security questions posed
  - Consider monthly security communications
  - Consider town halls
  - Praise employees (awards) who engage IS or compliance

Practical Consideration
Training Leadership

- Company leadership must understand IS risk
- Companies with security issues face unprecedented levels of federal and state enforcement
  - Likely subject to state law even if HIPAA inapplicable
- Private plaintiff class actions
  - Nominal damages provisions
  - HIPAA often used as a standard of care
- Contractual Damages
  - Cost of breach: Average of $201 per record affected ($398 per health care record)
  - Total costs rise to hundreds of millions
- Minor incidents now have a big effects on shareholder value and reputation
  - Incident effect largely dependent upon response

EPSTEIN BECKER GREEN

Interface of legal requirements with practical considerations

The Security Rule: In the Breach Age

- The Security Rule compatible with good IT security practices
  - Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of ePHI
  - Compliance, product development, legal, and IT all have a role
- Legal counsel must be involved
  - HIPAA is a legal standard not an IT standard
    - Requires sophisticated application of fact to law and assumption of risk based on cost-benefit analysis
- No compliance program or environment is "secure"
  - Preserve privilege to the extent possible

EPSTEIN BECKER GREEN

Practical Consideration
No Such Thing as HIPAA Compliant

- The "HIPAA Compliant" misnomer
  - Required and addressable implementation specifications
    - Risk Assessment (required)
    - Encryption (addressable)
  - No widget is HIPAA compliant until assessed in your environment
- Very few articulated controls
  - Organization specific

EPSTEIN BECKER GREEN

Practical Consideration
Be Careful Who You Hire

- Watch out for vendors who use the HIPAA risk assessment as a foot in the door to sell products
  - Consider policy where different vendors used for assessment and mitigation
- Do not allow non-legal vendors to make legal conclusions of compliance with law
  - Legal review prior to publishing of any report

EPSTEIN BECKER GREEN

Practical Consideration
Look for Standardization

- HIPAA is a non-prescriptive standard.
  - The controls implemented to safeguard information based on cost-benefit analysis and size and sophistication of entity
  - Required vs Addressable requirements
  - Data breach litigation has the benefit of hindsight
- Move from ad hoc security management program to a more defensible prescriptive standard
  - HITRUST, ISO, NIST CyberSecurity Framework

EPSTEIN BECKER GREEN

Practical Consideration
Response Plan

- It's not if… it's when: in a breach situation response time and response effectiveness critical
- Incident response plan:
  - Multidisciplinary
    - Must respond effectively while protecting organization
    - Chain of command
    - Articulated responsibility
  - Prepared
    - Clear protocol for triggering response team
    - Arrange for vendors before an incident happens
    - Understand reporting obligations

EPSTEIN BECKER GREEN

Practical Consideration
A Breach Is Not A Law School Hypo

- You cannot remove common sense from the equation
  - A data breach investigation is not an exercise in imagination
  - Must be grounded in fact through forensics and investigation
- Hire sophisticated counsel

EPSTEIN BECKER GREEN

Practical Consideration
Business

- The Privacy Rule requires BAAs be signed with any downstream BA.
- Business partners often the weakest link in IT security
  - Diligence to ensure adherence to BAA, other contractual obligations, and solid security
    - Would you buy this company?
    - What controls are most important to you?
  - Off-shore partners
    - Development, support, call centers etc.
  - Indemnification and financial footing

EPSTEIN BECKER GREEN

Practical Consideration
If You Sign A Contract HIPAA Applies

If you sign a BAA the provisions of the Privacy and Security Rules are applicable to you

- Days of "If Applicable" coming to end

EPSTEIN BECKER GREEN

Questions?

Adam Solander

Member of the Firm

asolander@ebglaw.com

202.861.1884

EPSTEIN BECKER GREEN

EPSTEIN
BECKER
GREEN

Thank you