HIPAA Auditing Update

TACUA 2015 Annual Conference
March 4, 2015

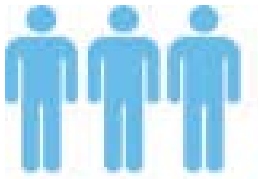
Your Presenters

Mike Cullen, Senior Manager, Baker Tilly
CISA, CISSP, CIPP/US

- Leads the firm's Higher Education Technology Risk Services team, focused on IT risk consulting and internal auditing.
- Performs IT risk assessments and audits, developed information privacy and security programs, performed ethical hacking of IT systems, and conducted digital forensic investigations.
- Presents to a variety of audiences, including ACUA, various IIA chapters and regional conferences, and at multiple universities.

Baker Tilly

BAKER TILLY



Over 2500 employees

12th

One of the largest professional services firms in the US.

9 out of 10

clients agree that Baker Tilly is proactive in meeting their needs

With locations in

TWENTY NINE

cities, we are always nearby

Baker Tilly Higher Ed Services

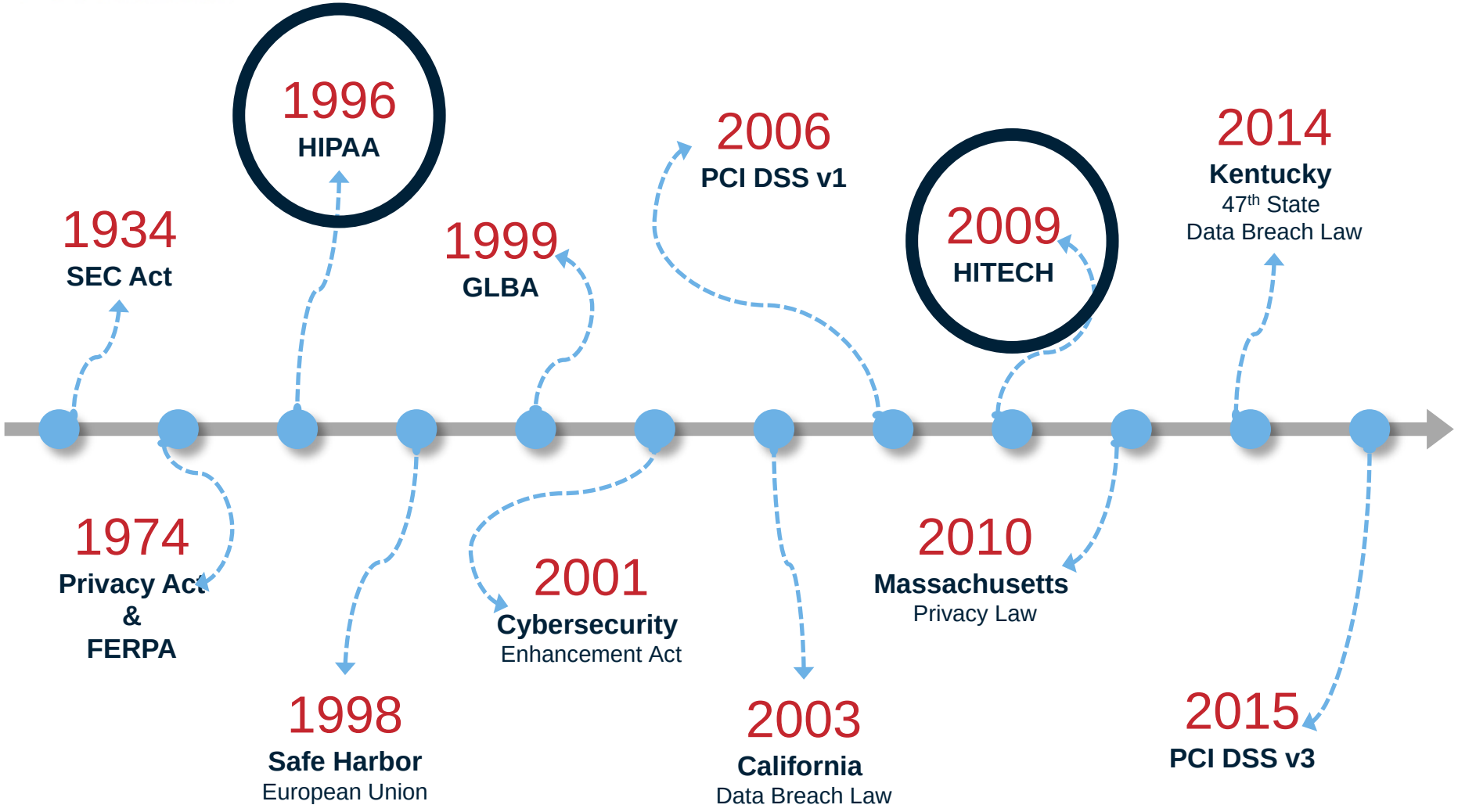
- Internal Audit
- Research and Grants Compliance
- Technology Risk and Cybersecurity
- Construction Risk Management
- Regulatory Compliance (e.g., HIPAA)
- Financial Statement Audit
- Single Audit
- Financial Ratios
- Resource Optimization

Objectives

- Highlighting the latest developments with HIPAA rulemaking and the OCR's planned audits of covered entities (CE) and business associates (BA)
- Discussing key areas of HIPAA compliance that institutions should review
- How Internal Audit can assist with the HIPAA security risk assessment for their institutions, whether as a CE or BA

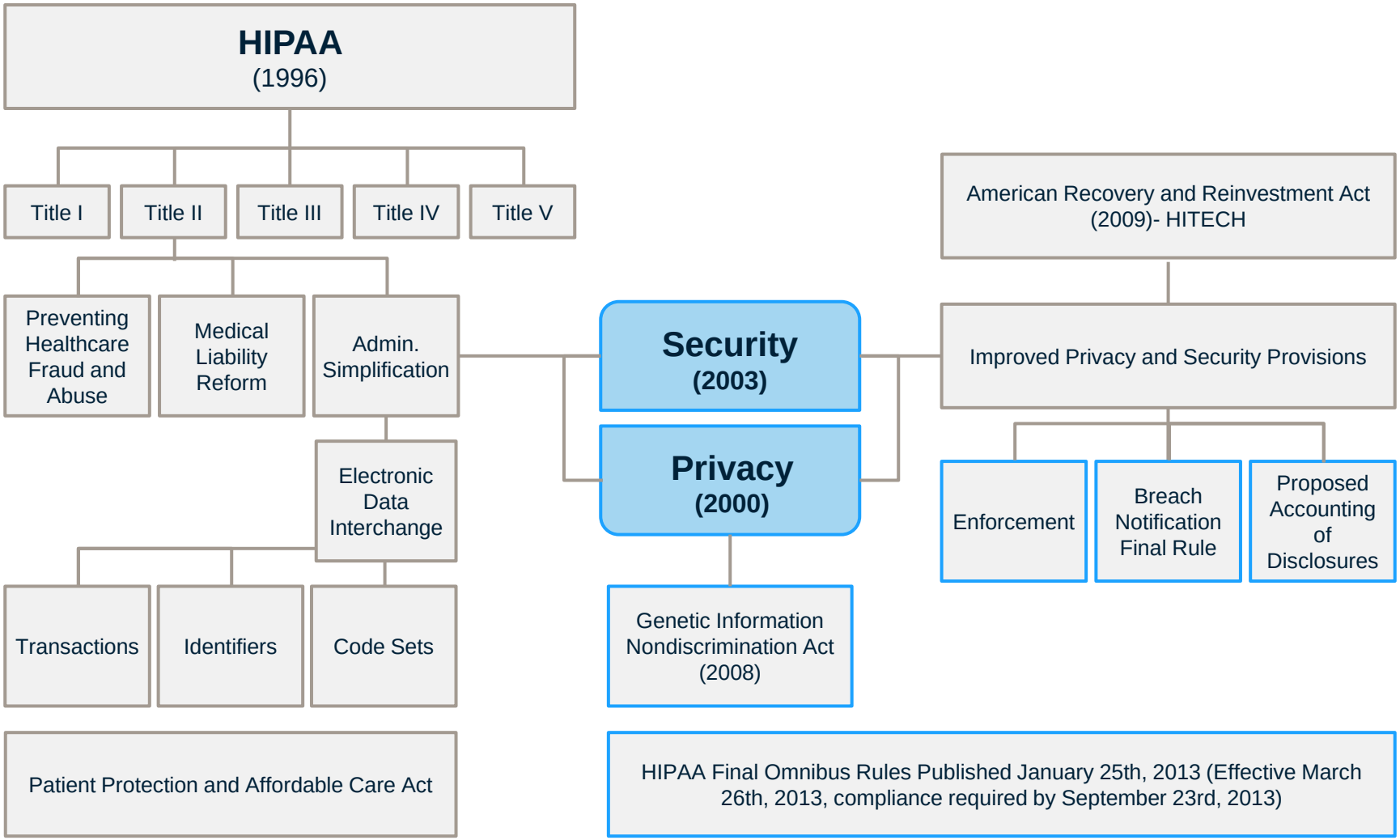
HIPAA
overview

Regulatory response over time



7

Brief history of HIPAA



Who must comply?

Covered Entities

- "Health plans, health care clearinghouses and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards"

Who must comply?

Business Associate:

- "A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate"

Who must comply?

Hybrid Entity

- "A single legal entity that is a **covered entity**; whose business activities include both covered and non-covered functions; and that designates health care components in accordance with HIPAA requirements"

Hybrid Entities Must:

- Designate the health care component
- Health care component complies with all requirements
- Create separations from the non-covered functions
- Ensure only limited allowed disclosures between health care component and non-covered functions, including workforce members with duties on both sides

Hybrid Entity

Advantages

>Limit scope of HIPAA compliance

>Target training and procedures to only health care component

>Include services as the health care component to share PHI without BAAs

Disadvantages

>Effort to identity and define health care component

>Create additional separations from the non-covered functions

>Limited disclosures outside of health care component still must be tracked

>Customer/partner road blocks when dealing with non-covered functions

>Challenges with common physical space and computer systems

Hybrid Entities & Research - NIH

- Research components of a hybrid entity that function as health care providers and conduct certain standard electronic transactions must be included in the health care components and be subject to the Privacy Rule
- Research components that function as health care providers, but do not conduct these electronic transactions may, but are not required to, be included in the health care components.
- The hybrid entity is not permitted to include in its health care component, a research component that does not function as a health care provider or does not conduct business associate-like functions. As such authorizations are generally required for use or disclosure of PHI for research purposes.

What does this mean for you?

CEs

Covered entities should:

- Understand BA compliance, up- and downstream
- Build collaboration and understanding with the BAs beyond the agreement
- Complete a HIPAA Security Risk Assessment

BAs

Business associates should :

- Understand CE expectations, as documented in the Business Associate Agreement (BAA)
- Ensure HIPAA compliance for downstream Bas
- Complete a HIPAA Security Risk Assessment

HIPAA

latest developments

Latest Developments

- BA Increased Compliance Requirements
- Omnibus Rule
- Enforcement
- Breach Notification Rule
- OCR Audits
- Emerging Risks

BA Increased Compliance Requirements

- All provisions of the Security Rule are now applicable
- BAs can be directly liable for HIPAA noncompliance
- BAs are required to have appropriate agreements in place with subcontractors who access EPHI
- Breach risk analysis is more comprehensive than the previous “harm threshold”
- Requirement to provide a copy of EPHI to a covered entity or individual upon request
- Requirement to maintain an accounting of disclosures

Omnibus Rule

- Subcontractors to CEs are defined as BAs, as such they require Business Associate Agreements (BAA)
- Defined PHI as individually identifiable health information that is:
  - Transmitted or maintained in electronic media
  - Transmitted or maintained in any other form or medium
- PHI excludes individually identifiable health information in the following:
  - FERPA educational records
  - FERPA records made or maintained by a physician, psychiatrist, psychologist, or other recognized professional
  - Employment records held by a CE
  - A person deceased for more than 50 years

Omnibus Rule: PHI's 19 items

- Names
- Geographic subdivisions smaller than a state
- All elements of dates (except year)
- Telephone numbers
- Fax numbers
- Email addresses
- SSN
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers
- Web URLs
- IP Address numbers
- Biometric identifiers
- Full-face photographs
- Any other unique identifying number, characteristic, code
- Individually identifying genetic information

Omnibus Rule

- Increased civil money penalties

Violation Category	Each Violation	Max Violation of Identical Provision in Calendar Year
(a) Did not know	$100 - $50,000	$1,500,000
(b) Reasonable cause	$1,000 - $50,000	$1,500,000
(c)(i) Willful neglect - corrected	$10,000 - $50,000	$1,500,000
(c)(ii) Willful neglect – not corrected	$50,000	$1,500,000

Enforcement - Columbia and New York Presbyterian

- Findings:
  - Columbia failed to conduct an accurate, and thorough risk analysis that incorporates all IT equipment, applications and data systems utilizing EPHI, including the server accessing NYP-EPHI.
  - Columbia failed to implement processes for assessing and monitoring IT equipment, applications and data systems that were linked to NYP patient databases prior to the breach incident and failed to implement security measures sufficient to reduce the risks of inappropriate disclosure to an acceptable level.
- Results
  - $1.5M for Columbia
  - Corrective Action Plan required for 3 years

Enforcement – Idaho State University

- Findings:
  - EPHI of approx. 17,500 patients was unsecured for at least 10 months after firewall was disabled
  - ISU risk assessments of clinics were incomplete and inadequately identified potential risk and vulnerabilities
- Results
  - $400,000 fine
  - Corrective Action Plan

Breach Notification Rule

- Defines breach (45 CFR § 164.402) as the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI
- An unauthorized acquisition, access, use, or disclosure of PHI (with enumerated exceptions) is presumed to be a breach unless the covered or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.
- This risk assessment must address at least the following factors:
  1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  2. The unauthorized person(s) who used the PHI or to whom the disclosure was made;
  3. Whether the PHI was actually acquired or viewed; and
  4. The extent to which the risk to the PHI has been mitigated.

Breach Notification Rule

- Exceptions:
  1. any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within the scope of authority, and if it does not result in further impermissible use or disclosure
  2. any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information is not further impermissibly used or disclosed
  3. a disclosure of PHI where a covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain the information

2014 HIPAA Breach in Texas

BAKER TILLY

http://www.healthcareinfosecurity.com/biggest-health-data-breaches-in-2014-a-7705

OCR Audits Phase 1

- Only 13 of the 115 organizations audited had no findings
- 58 of 59 healthcare providers had at least one finding or observation in the area of security
- Most common cause of findings was the CE was unaware of the requirement

Privacy
• Notice of Privacy Practices; • Access of Individuals; • Minimum Necessary; and, • Authorizations.

Security
• Risk Analysis; • Media Movement and Disposal; and, • Audit Controls and Monitoring.

OCR Audits Phase 2

- Timing was 2014, now delayed until ????
- Security risk assessments and breach notification will be key areas of focus for the audits
- Vet the audit protocol (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html)
- Inventory all current business associates
- Document and over-document; most audits are done via “desk audits” or review of documentation alone
- If you are selected, don’t ignore the federal government

Emerging Risks

- Cloud computing
- Mobile devices

HIPAA security

risk assessment

What is it?

HIPAA security risk assessments:

- Trace the flow of PHI inside and outside the organization
- Focus on four critical areas: processes, people, technology and governance
- Help organizations understand the level of risk, determine how to manage risk and help them target their main areas of risk

Scope: HIPAA security safeguards

Administrative safeguards

- Security management
- Security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plans
- Evaluation
- BA contracts

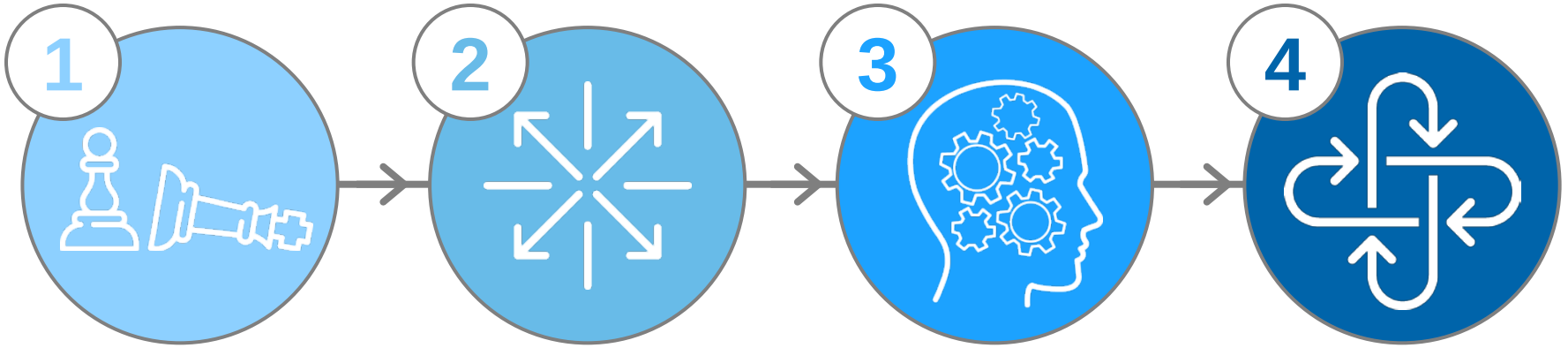
Technical safeguards

- Access control
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security

Physical safeguards

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

Key phases



PLAN PROJECT

Define in scope systems
Review policies and procedures
Review past and present projects
Build understanding of the PHI environment

DETERMINE RISKS

Conduct interviews with key stakeholders
Identify risks and vulnerabilities of PHI the organization creates, receives, maintains or transmits

ANALYZE GAPS

Evaluate risks and vulnerabilities in administrative, technical and physical safeguards
Assess security measures
Determine the risks' impact and likelihood

PRESENT RESULTS

Document findings related to threats and vulnerabilities
Document corrective action plans
Review results with key stakeholders

Table 1: Taxonomy of Operational Risk

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

Software Engineering Institute – Taxonomy of Operational Cyber Security Risks Version 2

Lessons learned

Common mistakes include:

- Incomplete ePHI inventory and inadequate scoping of the assessment
- Lack of strong, executive sponsorship
- Poor understanding of the HIPAA Security Implementation Specifications
- Inability to effectively prioritize remediation activities
- Assessor lacks adequate knowledge and independence

HIPAA

breach notification and incident response

Why does your institution need an Incident/Breach Response Plan?

- It is not a matter of if your institutions will have an incident or breach, it is a matter of when
- Decentralized organizations with numerous stakeholders increase the likelihood of ad hoc responses
- Inappropriate or inadequate response can lead to reputational and financial damage

What is a Incident/Breach Response Plan?

- “Capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits” – ISACA

Why is Incident/Breach Response Important?

- Breaches are happening more frequency
- 2014 was a record year for breaches in the press/media
- Regulations require incidence/breach response plans
- http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Why is Incident/Breach Response Important?

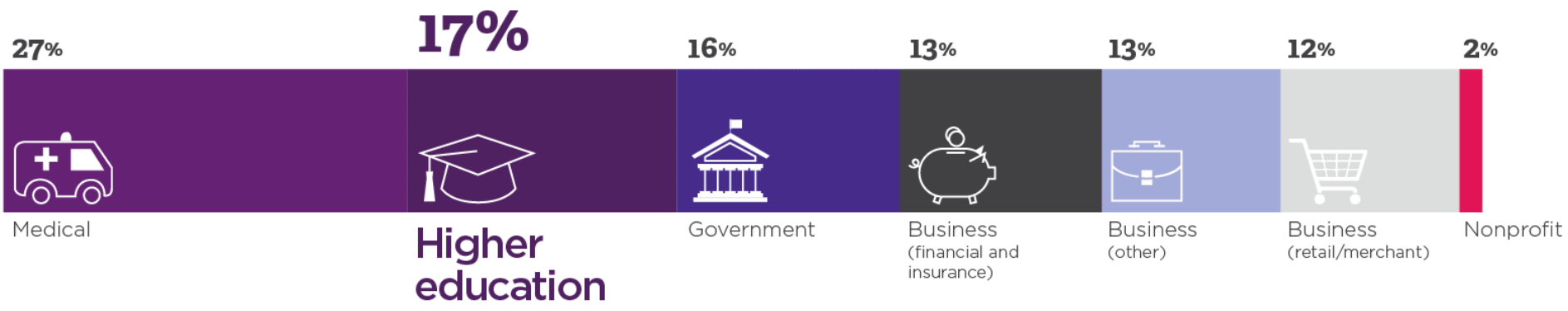
BAKER TILLY

Banner®
DATA
DEFENSE

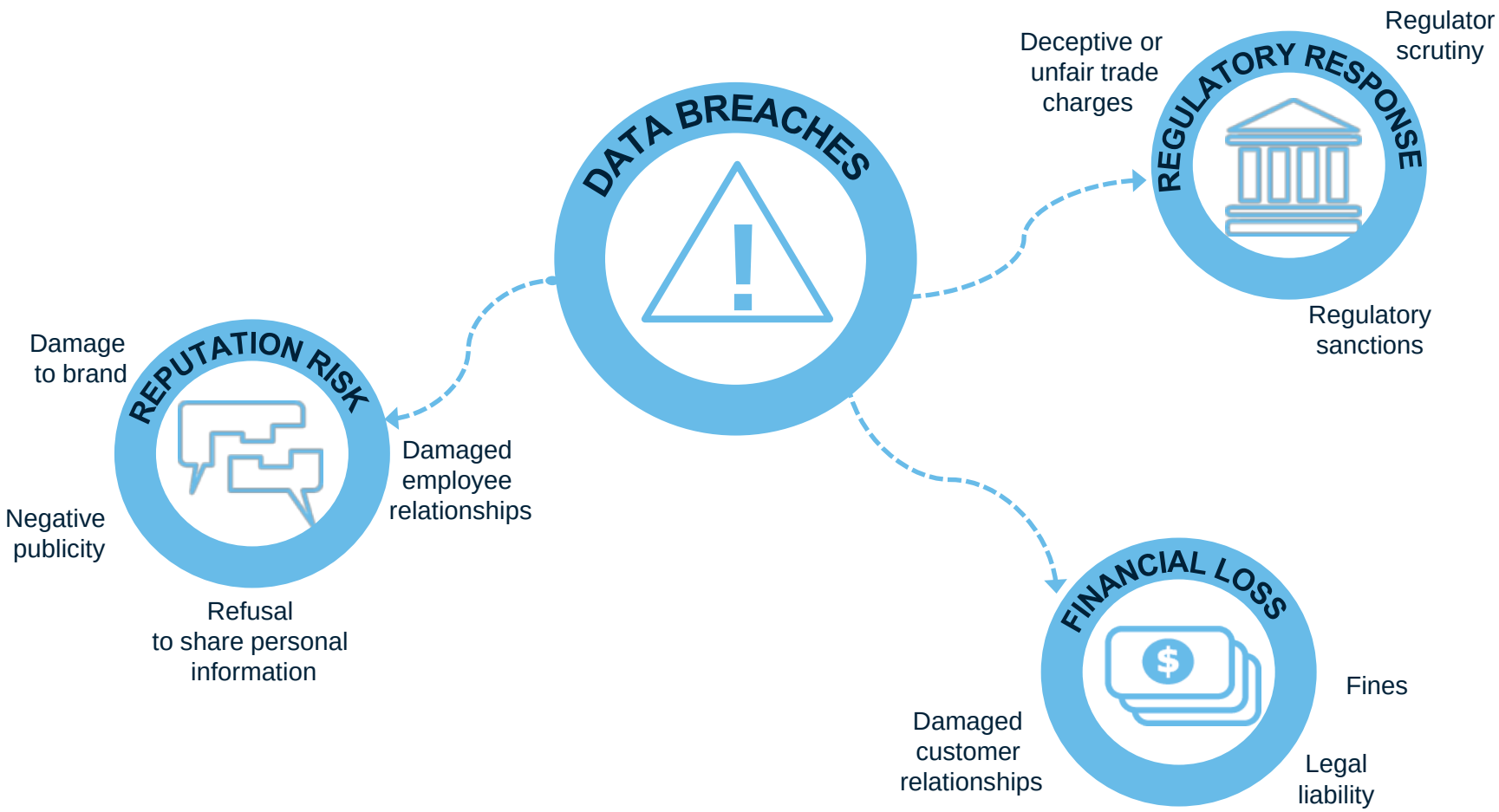
The higher education industry accounts for 17% of all reported data breaches,

second only to the medical industry with 27%.

2005–2014 Privacy Rights Clearinghouse, https://www.privacyrights.org/data set

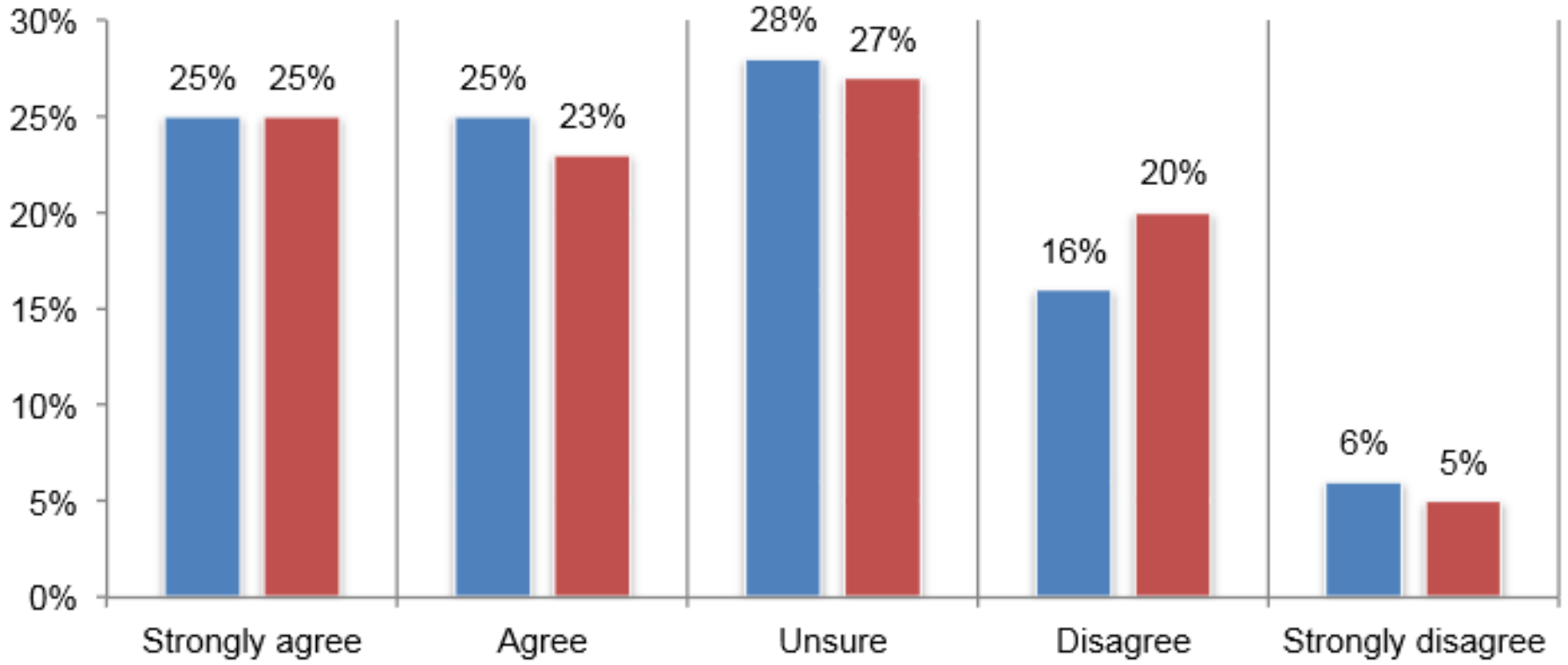


Impacts of Data Breaches



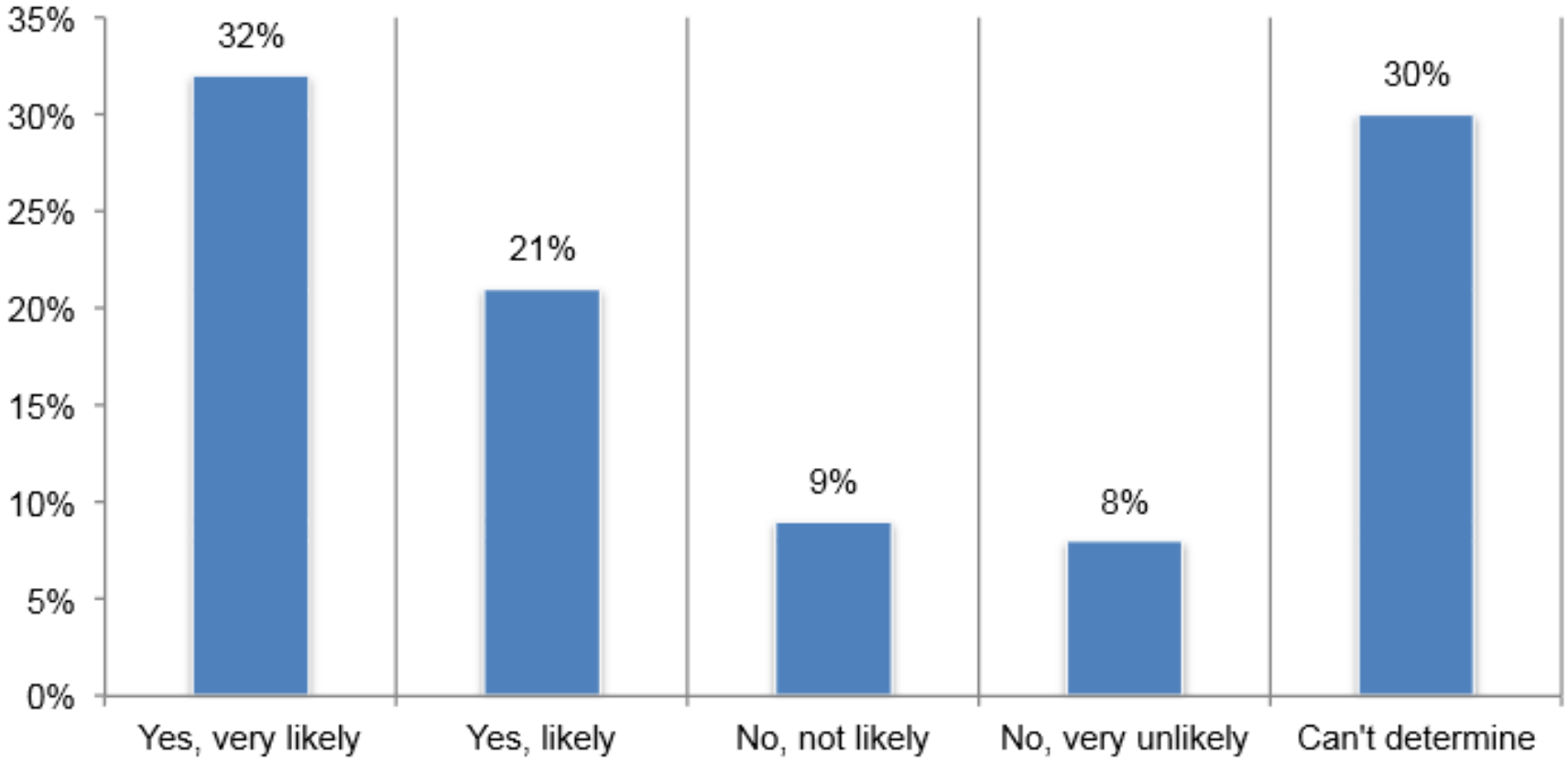
BAKER TILLY

Figure 4. I would find another healthcare provider if I had concerns about the security of my medical records or if they were stolen



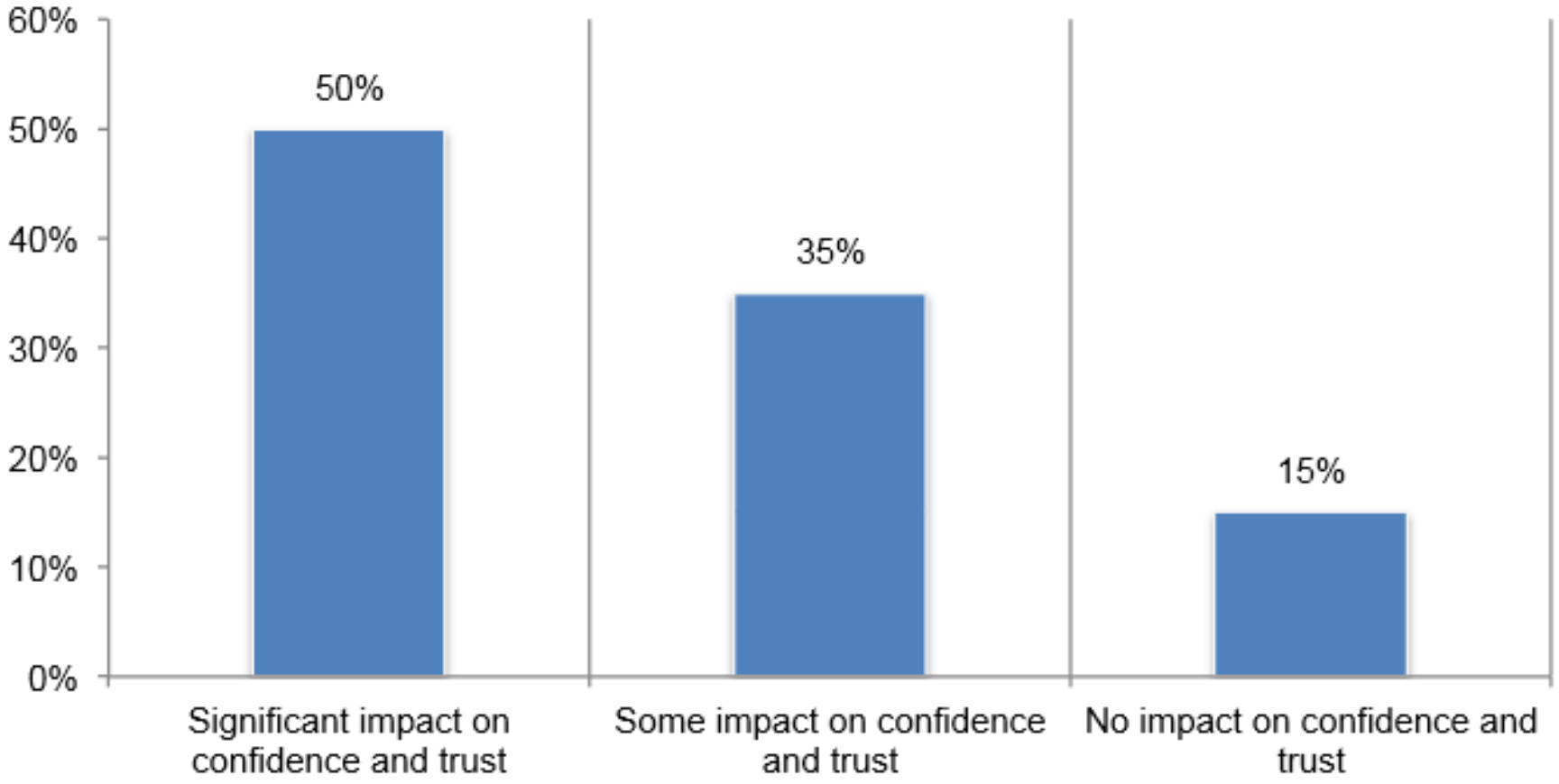
BAKER TILLY

Figure 8. Did your healthcare provider's negligence cause or contribute to your medical identity theft?



BAKER TILLY

Figure 9. If yes, did it diminish your trust in your healthcare provider?



- What Is a Breach Requiring Notification?
  - Minimum Necessary Violations May Require Breach Notification
  - Nature and Extent of PHI Involved
  - Unauthorized Person Who Used PHI
  - Whether PHI Was Actually Acquired or Viewed
  - Extent to Which Risk to PHI is Mitigated
  - Exceptions

- Notification to Individuals
  - Timeliness
  - Content of Notification
  - Notification Methods
- Notification to the Media
- Notification to HHS
- Notification by a Business Associate

State Laws

- 47 states, DC, Guam, Puerto Rico, US Virgin Islands
  - Exception Alabama, New Mexico, South Dakota
  - **Kentucky joined the club April 11, 2014**

- Texas law defines “sensitive personal information”:
  - 1) the physical or mental health or condition of the individual;
  - 2) the provision of health care to the individual; or
  - 3) payment for the provision of health care to the individual.
  - A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act
  - Encryption provides safe harbor (unless encryption key is breached)

State Laws

- The National Conference of State Legislatures maintains a list of State Security Breach Notification Laws with links to the text of each law. Check the list regularly as the state laws continue to change.

- A substantial number of reported breaches have involved non-profit universities and health systems. See Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities)

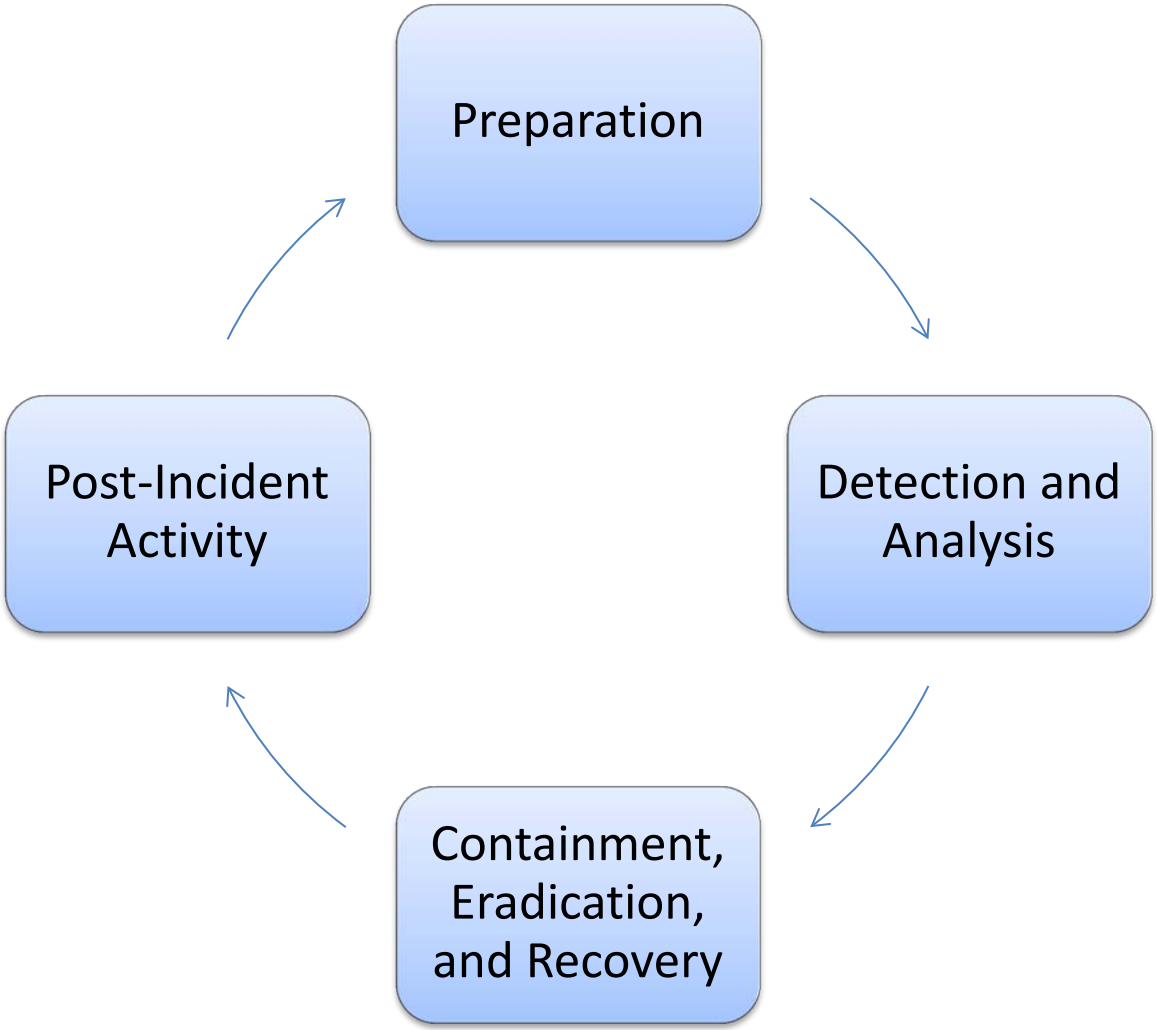
Incident/Breach Planning
Key Components

- Policy – establishes goals and vision for the breach response process, defined scope (to whom it applies and under what circumstances), roles and responsibilities, standards, metrics, feedback, remediation and requirements for awareness training
- Plan – covers all phases of the response activities
- Procedures – derives from the Plan and codifies specific tasks, actions and activities that are part of the breach response effort.

Why Should an Incident/Breach Response Plan be Audited?

- Ensures that the plan contains accurate, current information
- Allows the response process to be assessed and fine-tuned
- Identifies potential issues in advance; before the breach occurs
- Should a breach subsequently occur, it allows the process to operate more efficiently

What is the purpose of a Incident/Breach Response Plan?



What Should Your Incident/Breach Response Plan Contain?

- Individuals/team that will lead the breach response process and make the final determination that an actual breach has occurred
- Emergency contacts
- Reporting a breach:
  - Internal reporting system to alert legal, senior management, communications, employees and others
  - External reporting to customers, business partners, public at large
- Information on relevant regulatory and law enforcement agencies that must be contacted
- Steps required to assess scope of breach and preparation of response (including containment, eradication and recovery)
- Post-mortem assessment, remediation, ongoing training

What Roles Should Your Incident/Breach Response Plan Contain?

- Designated Incident Lead
  - One individual (and backup) has been designated to coordinate the response
  - Acts as go-between for management and the response team
  - Typically someone from Legal
  - Coordinates efforts among all groups, notifies appropriate people within the company and externally, documents the response, identifies key tasks, and estimates remediation costs
- Who makes the call?
  - Consists of representatives from IT/Security, Legal, and Senior Leadership
  - Once the facts are gathered, the most senior-level executive makes the determination that a breach has/has not occurred, and "breaks the glass" to execute the response plan

Emergency Contacts and Internal Reporting System

- Emergency Contact List should include:
  - Representative(s) of executive management team
  - Legal, privacy & compliance
  - Operations (Security & IT)
  - Customer Service and/or HR
  - Communications/ Public Relations
  - Representatives of third-party vendors
  - Outside Experts
- Incident Response Plan should designate structure of internal reporting system

Reporting a Breach

- There should be a well-known mechanism for all employees to report a suspected breach of sensitive information
- There should be recurring training for all staff, that includes:
  - What constitutes a breach
    - HIPAA has 19 types of PHI
  - What does NOT constitute a breach
    - Accidental disclosure
  - What are the appropriate communications channels should a breach be suspected
- Plan should be tested/rehearsed (table-top testing) not less than once per year

Assessing the Breach and Response

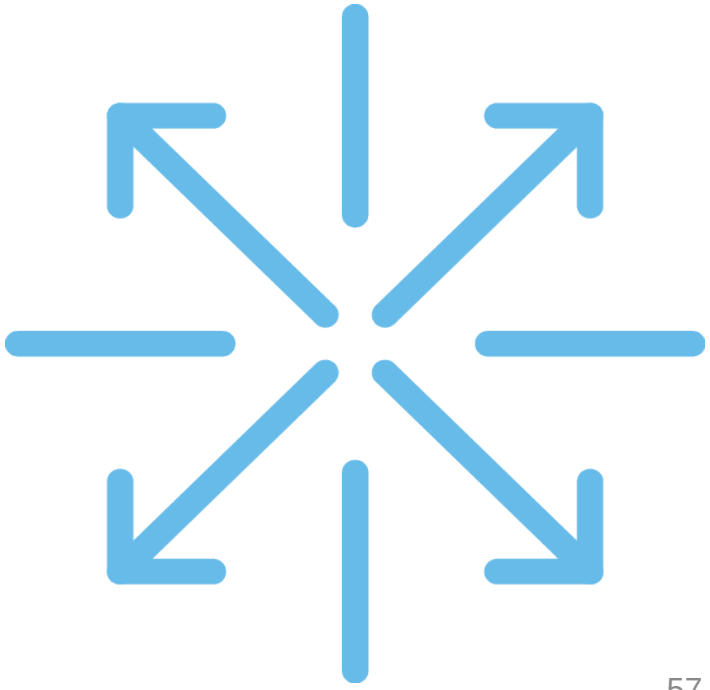
Incident Plan should contain steps necessary to contain the breach and to conduct a preliminary internal assessment of the scope of the breach.

Consider:

- Isolating the affected system to prevent further release
- Reviewing/activating auditing software
- Preserving pertinent system logs
- Making back-up copies of altered files to be kept secure
- Identifying systems that connect to the affected system
- Retaining an external forensic expert to assist with the investigation
- Documenting conversations with law enforcement and steps taken to restore the integrity of the system

Demonstrating

HIPAA compliance



Demonstrating compliance

How do you demonstrate compliance the OCR?

> Document and retain the risk analysis

> Consider using the OCR tools and templates

Key questions to ask:

> Have you identified the EPHI within your organization?

> What are the external sources of EPHI?

> What are the human, natural and environmental threats to information systems that contain EPHI

Demonstrating compliance cont.

Organizations should use the information to:

- Design appropriate screening processes.
- Identify what data to backup and how
- Address what data must be authenticated in particular situations to protect data integrity
- Determine the appropriate manner of protecting information storage and transmissions

Regulator Questions

Key questions that a regulator may ask:

- What approach did you use to conduct the HIPAA Security Risk assessment?
- Has an EPHI data inventory been created and data flows tracked?
- What are your vendor risk management practices?
- What are the human, natural and environmental threats to information systems that contain EPHI?
- How is EPHI on remote devices protected? Is encryption utilized?
- Describe your breach/incident management procedures? How are these coordinated with any third-party vendors?

Internal vs. external risk assessments

Internal

Pros

- Internal resources will know the entity better
- May be more cost effective if expertise is already in house

Cons

- Lack of true independence or perspective on risks

External

Pros

- External should have expert level knowledge
- Can provides perspective on similar clients

Cons

- External resources do not know the entity as well as internal

Attestation and certification

Service Organization Controls (SOC) 2 examinations

- Reports on controls of operations
- Security, Availability, processing integrity, confidentiality, privacy
- Consist of infrastructure, software, people, procedures and data
- Formal audit opinion
- Can be mapped to specific regulatory requirements and control frameworks (i.e. HIPAA Security Standards)

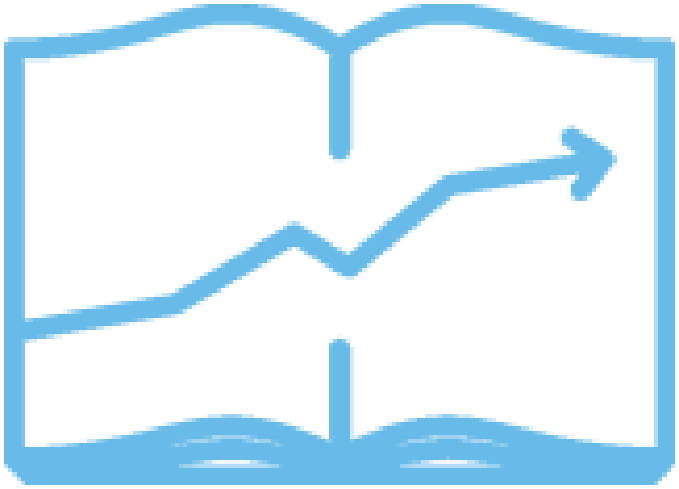
Health Information Trust Alliance (HITRUST)

- Common security framework that can be used by entities that create, access, store or exchange sensitive or regulated data

NO Real HIPAA Compliance Certification

Resources

for more info



Resources

- CERT (http://www.cert.org/incident-management/)
- EDUCAUSE (www.educause.edu)
- Higher Education Information Security Council, HEISC (https://wiki.internet2.edu/confluence/display/2014infosecurityguide/)
- ISACA (www.isaca.org)
- NIST (www.nist.gov)
- Department of Education Privacy Technical Assistance Center (PTAC) Data Breach Response Checklist (http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf)
- National Conference of State Legislatures (http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)
- Privacy Rights Clearinghouse Chronology of Data Breaches (http://www.privacyrights.org/data-breach/new)

Resources

- Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule (http://privacyruleandresearch.nih.gov/pr_02.asp)
- Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Years 2011 and 2012 (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf)
- Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Years 2011 and 2012 (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereport2011-2012.pdf)
- BakerHostetler Data Breach Charts (http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf)
- Mintz Levin Health Law & Privacy Matters Blog (http://www.healthlawpolicymatters.com/)
- The Practical Guide to HIPAA Privacy and Security Compliance, Second Edition, Herold and Beaver

Presenter Contact Info

Mike Cullen

mike.cullen@bakertilly.com

703-923-8339

Required disclosure and Circular 230 Prominent Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Pursuant to the rules of professional conduct set forth in Circular 230, as promulgated by the United States Department of the Treasury, nothing contained in this communication was intended or written to be used by any taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer by the Internal Revenue Service, and it cannot be used by any taxpayer for such purpose. No one, without our express prior written permission, may use or refer to any tax advice in this communication in promoting, marketing, or recommending a partnership or other entity, investment plan or arrangement to any other party.