The Twenty- Eighth National HIPAA Summit

HIPAA/HITECH Security Basics

March 4, 2019

Presented by

John Parmigiani

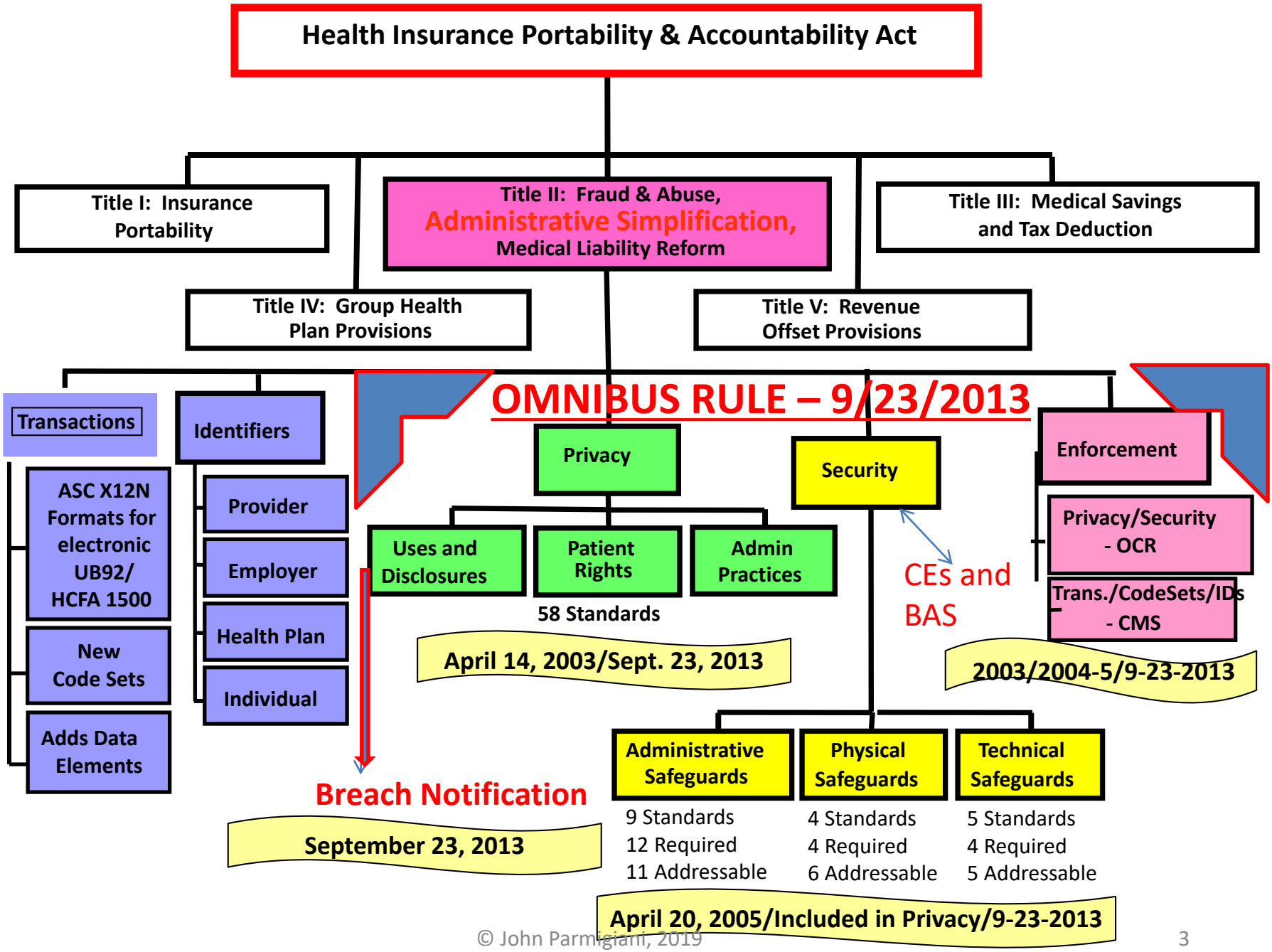
President

John C. Parmigiani & Associates

HIPAA* / HITECH**

**Health Information Technology for Economic and Clinical Health Act

*Health Insurance Portability and Accountability Act



Federal Regulatory Requirements Timeline

Safeguard Legislation and Enabling Regulations:

- Safeguards legislated in 1996 in the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act (HIPAA)
- HIPAA Privacy Rule required compliance by April 14, 2003 (Small health plans had additional year)
- HIPAA Security Rule Required compliance by April 20, 2005 (Small health plans had additional year)
- **Safeguards modified in February 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) legislated as part of the American Recovery and Reinvestment Act (so-called *Stimulus Bill*)**
  - ***Made the HIPAA Security Rule also apply to Business Associates as well as Covered Entities***
- HITECH Act Breach Notification Interim Final Rule required compliance by February 18, 2010
- HITECH Act Modifications of HIPAA Privacy and Security Rules and Breach Notification Rule (*The Omnibus Rule*) required compliance by September 23, 2013.

Government's Intent: Title II: Subtitle F Administrative Simplification ("HIPAA")

- Reduce healthcare administrative costs by standardizing (format and content) electronic data interchange (EDI) for claims submission, claims status, referrals, eligibility, COB, attachments, etc.- Foster E-Commerce - can also be used to streamline ordering and paying for supplies and services
- Establish patient's right to Privacy
- Protect patient health information by setting and enforcing Security Standards
- Promote the attainment of a complete Electronic Medical Record (EMR) and put the US on the path to Electronic Healthcare **(eHealth)**

HIPAA/HITECH Security Compliance Objective

Securing *protected health information* so that it is not impermissibly accessed, disclosed, or used by unauthorized persons or processes.

Accomplished through

- Conducting and periodically reviewing and updating an analysis of risk pertaining to PHI.
- Identifying risk mitigation strategies and shaping safeguard policies and procedures based on risk analysis findings.
- Creating and Training workforce members on safeguard policies and procedures.
- Documenting all safeguard activities, actions, and assessments.
- Maintaining ongoing vigilance. - Administrative and Technical Evaluation

HIPAA, HITECH, MU and the Path to E-Health

- **HIPAA Transactions and Code Sets**
- **HIPAA Privacy Rule**
- **HIPAA Security Rule**
- **National Provider Identifier**
- **HITECH / Omnibus Rule**
  - Privacy
  - Security
  - Breach Notification
- **Meaningful Use***
  - Standards
  - Certification
- EMRs
- EHR
- HIE – being able to securely share ePHI

HIPAA Administrative Simplification

Strengthened requirements and enforcement

E- Health

*David Blumenthal, MD, ONC – on meaningful use, Dec. 7, 2009: ***"It's not the technology that's important, but its effect. Meaningful use is not a technology project, but a change management project. Components of meaningful use include sociology, psychology, behavior change, and the mobilization of levers to change complex systems and improve their performance."***

E-Health Requirements

- **Heavily dependent on Privacy and Security: Key word is "*Trust*"**
  - Trusted relationships and communications
  - Physicians become the trusted party
  - Real-time interoperability for effectiveness and efficiency
  - Accuracy (**integrity**) of ePHI [for patient safety and healthcare delivery quality] to those systems and people with a "need to know" (**confidentiality**) and accessible when they need it (**availability**)… *"only the right people get to the right information at the right time"*
  - Therefore, the need for:
    - **Authentication**
    - **Access controls to allowed data**
    - **Monitoring and recording access requests**

Why is Protecting Patient Data so Important?

- People choose to disclose their most intimate information in order to get healthy
- Caregivers earn their trust by guaranteeing privacy
- Privacy is assured by properly protecting systems and information
- Breaches undermine patient confidence
- No confidence and people avoid treatment, lie or omit information, opt-out, and potentially get sicker
- Medical identity theft is on the rise
- Increased medical device use opens patients to safety risks through life-threatening cyber changes and malware infestation
- Privacy and security are integral components of delivering safe and effective health care

What is Covered?

***Health Information* as defined in section 1171 of the Act**

- *Any information*, whether oral or recorded in any form or medium, that
- is *created or received* by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and
- relates to the past, present, or future *physical or mental health (psychotherapy "session" notes)* 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 the individual*, or
- with respect to which there is reasonable basis to believe that the information can be used to identify the individual

Protected Health Information (PHI)

What is *protected health information*(PHI)?

Any of 18 identifiers (identified in the HIPAA Privacy Rule) that can pinpoint the identify of an individual associated with healthcare information such as in a medical record at a healthcare provider, in an insurance file at a health plan, or in the custody of a healthcare clearinghouse.

- **PHI can be in hard copy, electronic, or oral.**
- **HIPAA Privacy Rule (all PHI)**
- **HIPAA Security Rule (electronic PHI only)**

The Hippocratic Oath declares:

"Whatever, in connection with my profession, or not in connection with it, I may see or hear in the lives of men which ought not be spoken abroad I will not divulge as reckoning that all should be kept." **.....HIPAA is a bit more specific...**

Something to Keep in Mind

PHI should be seen by only those who are authorized to see it.

PHI should be heard by only those who are authorized to hear it.

PHI should by transmitted or shared with only those who are authorized to receive it.

- **Use and disclosure is limited to the minimum necessary.**
- **Reminder: Minimum necessary does not apply to treatment, payment, or healthcare operations.**

HIPAA Security Rule- Key Concepts

Flexible

Scalable

Technology Neutral

Comprehensive

What the HIPAA Security Rule Expects

- Ensure the confidentiality, integrity, and availability of all electronic PHI
- Protect against any reasonably anticipated threats and uses or disclosures that are not allowed by the Privacy Rule
- Mitigate these threats by whatever safeguards you believe can reasonably and appropriately be implemented in line with the Security Rule standards
  - Whether the standards are required or addressable, the safeguards should be based upon the organization's risk analysis and industry best practices
  - Must document your security decisions in light of your risk analysis; organizational size, complexity, and capabilities; cost to implement; and technical environment

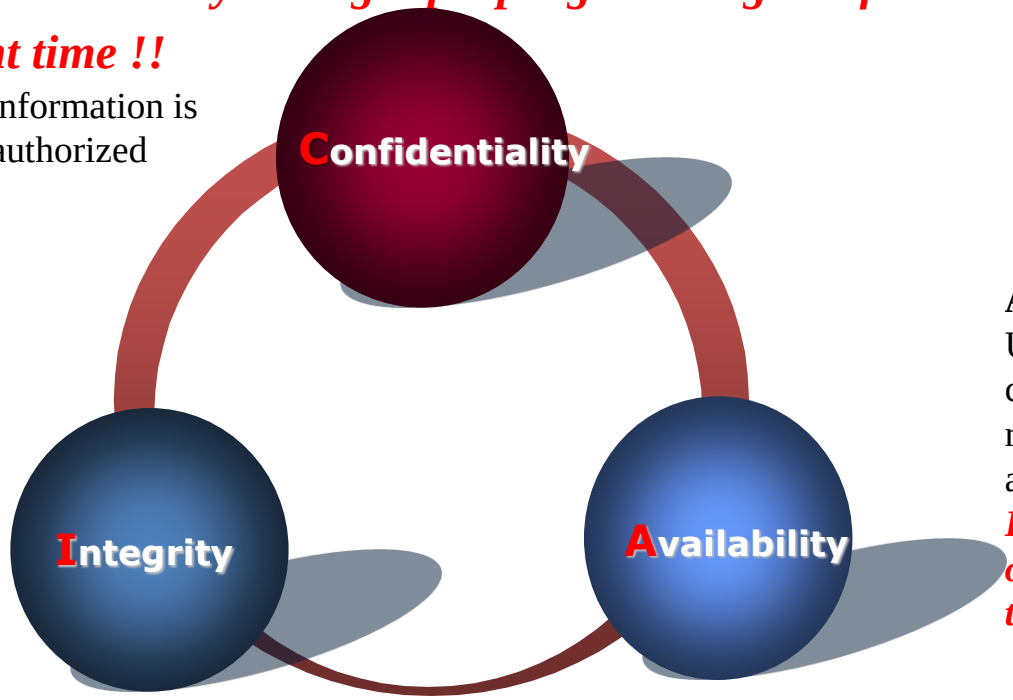
Information System Security

- Information System Security is designed to:
  - Protect systems and data against intrusion;
  - Prevent unauthorized access to or modification of information; and
  - Have information accessible to authorized users
  - Uphold the three primary corner stones of Information Security

making sure that only the right people get the right information at the right time !!

Confidentiality
Integrity
Availability

Confidentiality – Information is not disclosed to unauthorized personnel



Integrity – Protect information from unauthorized modification or destruction

Availability – Uninterrupted access to critical systems, resources, or data to authorized personnel

Ransomware is a form of breach that denies this key aspect

Can't have Privacy without Security!

Making Sure Health Information is Secure

Paper World

- Locks on doors
- Locks on file cabinets
- Storage in non-public areas
- Restricted access to areas

Electronic World

- Encryption
- Workstation security
- Audit controls
- Access control
  - *User ID and Passwords*
  - *Biometrics*
  - *Auto log-off*
  - *Restricted terminals*

HIPAA Privacy/Security Comparisons

Privacy

- Patient-centric
- PHI- electronic, paper, & oral
- Awareness & Training
- BA Contracts
- Privacy Officer(s)
- All aspects of delivering health care
- *Reasonableness* *

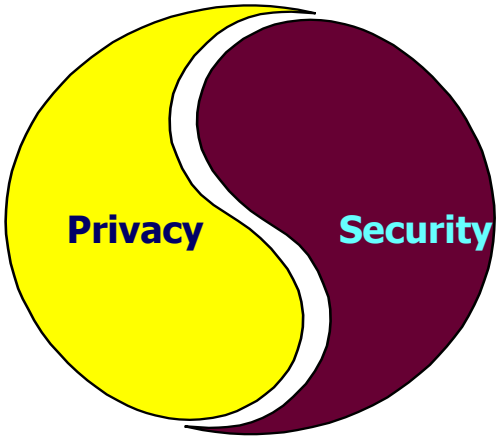
Security

- Organization (Covered Entity / Business Associate)-centric
- PHI- electronic
- Awareness & Training
- BA Contracts
- Security Officer(s)
- All aspects of delivering health care
- *Reasonableness* and Appropriateness*

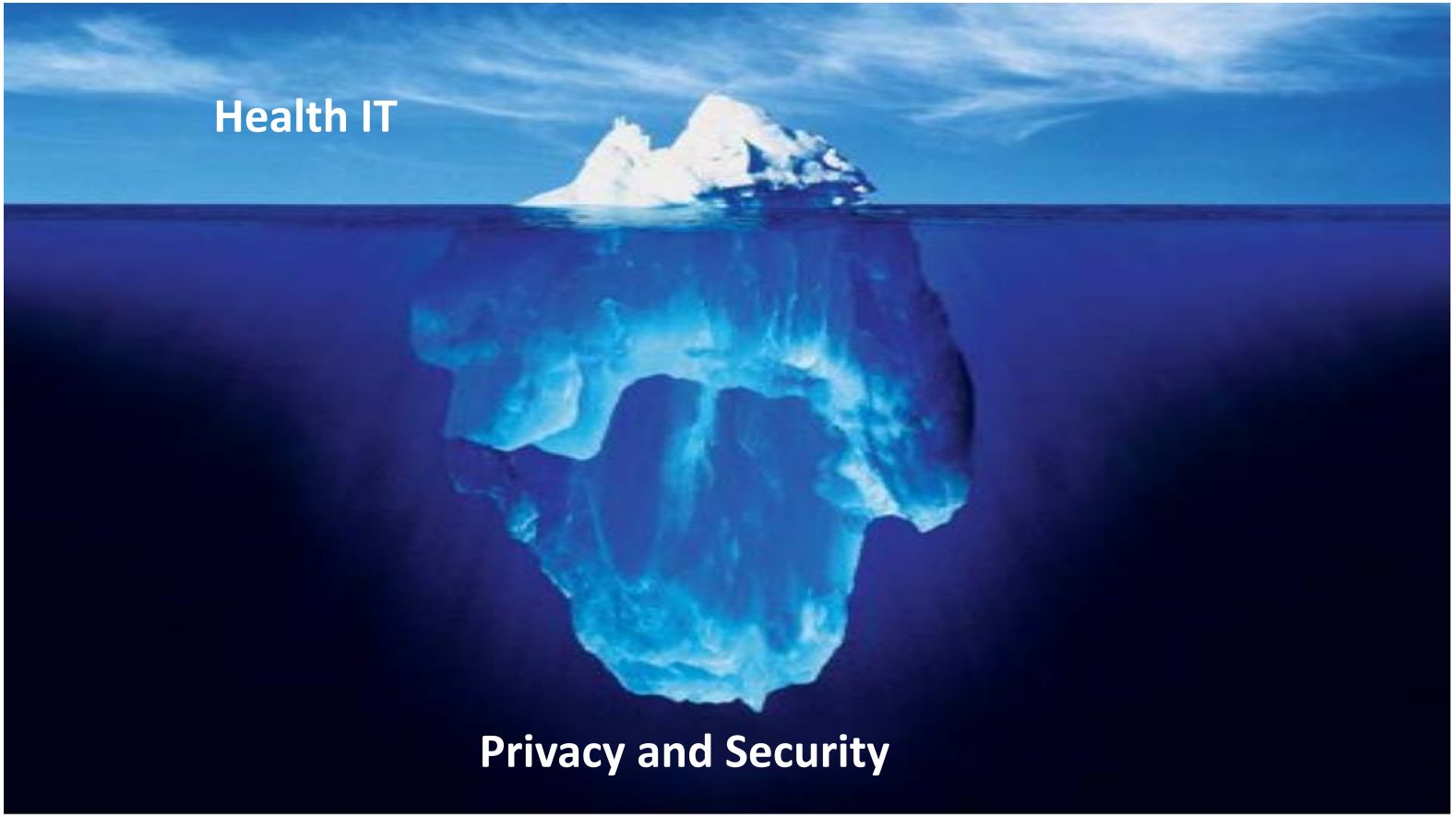
* 57 times in the Security Rule
356 times in the Privacy Rule

Serendipity Effect of Privacy Compliance

- Security and Privacy are inextricably linked
  - Can have Security by itself *but* cannot have Privacy without Security
  - Privacy has already necessitated a degree of security implementation and compliance because of its "reasonable safeguards" requirements to protect PHI as stated in the Privacy Rule



Privacy and Security is the Foundation for HIT



Accepted Security Principles

Repeated thoughtful use of these well-accepted principles reduces risk.

- Need to Know (minimum use)
- Least Privileges
- Separation of Duties
- Defense-in-Depth
- Security Equation

Security **=**

People **+**

Process **+**

Policy **+**

Technology **+**

[Common Sense]

HIPAA Security Standards

	Administrative	Physical	Technical
Standards [18]	9	4	5
Required [20] **Implementation Specifications**	12 (4)	4 (4)	4 (4)
Addressable [22] **Implementation Specifications**	11 (4)	6 (2)	5 (5)

(utilize a technical solution)

Organizational Requirements

Policies and Procedures and Documentation Requirements

The final rule was modified to increase flexibility as to how protection is accomplished. Emphasis is on **optimal blend of people and technology to provide good security**.

- ***Consider industry best practices.*** *(Approximately 40+ outlined in the rule as guidance)*

Addressable Implementation Specifications…

- Covered eternities must assess if an implementation specification is reasonable and appropriate based upon factors such as:
  - Risk analysis and mitigation strategy
  - Current security controls in place
  - Costs of implementation

- Key concept: "reasonable and appropriate"

- Cost is not meant to free covered entities from their security responsibilities

Addressable does not mean Optional!

Addressable Implementation Specifications

- If the implementation specification is reasonable and appropriate, then implement it

- If the implementation specification is not reasonable and appropriate, then:
  - Document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate

    or
  - Do not implement and explain why in documentation

Administrative Safeguards

Administrative actions and policies and procedures used to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the CE's/BA’s workforce in relation to the protection of that information.

Administrative Safeguards

(with Technical Solutions noted)

Standards	Sections	Implementation Specification	R/A	T
Security Management Process	164.308(a)(1)	Risk Analysis	R	
		Risk Management	R	
		Sanction Policy	R	
		IS Activity Review	R	
Assigned Security Responsibility	164.308(a)(2)		R	
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A	
		Workforce Clearance Procedures	A	
		Termination Procedures	A	
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	R	
		Access Authorization	A	**Y**
		Access Establishment and Modification	A	**Y**
Security Awareness and Training	164.308(a)(5)	Security Reminders	A	
		Protection from Malicious Software	A	**Y**
		Log-in Monitoring	A	**Y**
		Password Management	A	
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R	**Y**
Contingency Plan	164.308(a)(7)	Data Backup Plan	R	**Y**
		Disaster Recovery Plan	R	**Y**
		Emergency Mode Operation Plan	R	**Y**
		Testing and Revision Procedure	A	
		Applications and Data Criticality Analysis	A	
Evaluation	164.308(a)(8)		R	
BA Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	R	

*

*R=required; A=addressable; T=technical solution

Physical Safeguards

Physical measures, policies, and procedures used to protect a CE's/BA's electronic information systems, related buildings, and equipment from natural hazards, environmental hazards, and unauthorized intrusion.

Physical Safeguards

(with Technical Solutions noted)

Standards	Sections	Implementation Specifications	R/A	T
Facility Access Controls	164.301(a)(1)	Contingency Operations	A	
		Facility Security Plan	A	
		Access Control and Validation Procedures	A	**Y**
		Maintenance Records	A	
Workstation Use	164.310(b)	Documented procedures for system use	R	**Y**
Workstation Security	164.310(c)	Physical placement and control	R	**Y**
Device and Media Controls	164.310(d)(1)	Disposal	R	**Y**
		Media Re-use	R	**Y**
		Accountability	A	
		Data Backup and Storage	A	**Y**

*

*R=required; A=addressable; T=technical solution

Technical Safeguards

The technologies and policies and procedures for CE's/BA's use to protect electronic PHI and control access to it.

Technical Safeguards

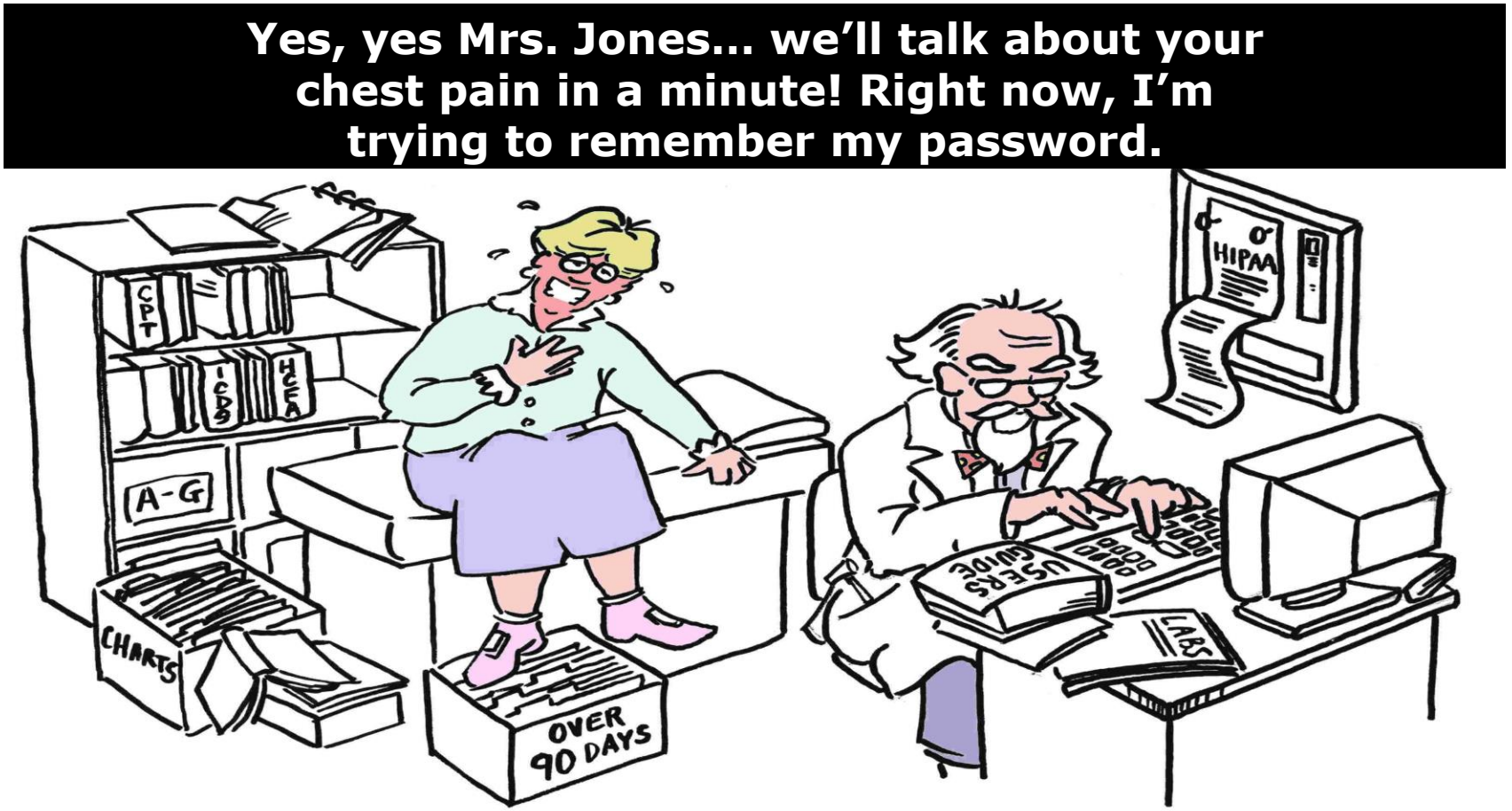
(with Technical Solutions noted)

Standards	Sections	Implementation Specifications	R/A	T
Access Controls	164.312(a)(1)	Unique User Identification	R	**Y**
		Emergency Access Procedure	R	**Y**
		Automatic Logoff	A	**Y**
		Encryption and Decryption	A	**Y**
Audit Controls	164.312(b)		R	**Y**
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic PHI	A	**Y**
Person or Entity Authentication	164.312(d)		R	**Y**
Transmission Security	164.312(e)(1)	Integrity Controls	A	**Y**
		Encryption	A	**Y**

*

*R=required; A=addressable; T=technical solution

But…
Security should never get in the way of delivering health care!



Regulatory Drivers: Privacy & Security (not just HIPAA)

Laws, regulations, draft bills, and accreditation practices related to information security are many and growing.

USA

- HIPAA/HITECH *
- FERPA
- 21 CFR Part 11
- 42 CFR Part 2
- PCI*
- GLBA
- SOX
- FISMA
- GINA (genetic info. now under Privacy Rule)
- 50 states (*Data Protection Acts*) + DC, Puerto Rico
- FTC Red Flags Rule*-to prevent ID Theft
- JCAHO
- NCQA
- OMB/NIST/CMS directives & guidance

***HCOs could be liable under these simultaneously**

International

- GDPR
- ISO/IEC 27000:2018
- Japanese Data Protection Law
- Canadian PIPEDA
- Basel II
- The UK Data Protection Act
- GCSX Code of Connection Compliance (UK)
- The German Federal Data Protection Act
- The New Zealand Privacy Act
- The Australian Privacy Act

Standard of due care principle for enforcement

Legal Basis for "Keeping Up with Technology"

The T.J. Hooper case:

- New Jersey coast (1928) - storm comes up,

  tug loses barge, and cargo of coal
- Plaintiff: Barge owner – captain of the tug (The T.J. Hooper) was negligent because he had no weather radio, which was relatively new but was seeing widespread use even though not mandated
- Defendant: Tug captain - didn't have the resources ($) to have a weather radio
- Decision (1932): Judge Learned Hand - Barge owner wins

  Rationale: to avoid negligence, keep up

  with technological innovations - they set the

  "standard of care" in the industry

Common Security Requirements

- The many standards associated with security have a strong commonality of features:
  - Protect **confidentiality** of sensitive data at rest and in transit
  - Restrict data access on need-to-know basis
  - Authentication/Access Controls/Audit Controls
  - Assure data **integrity**
  - Business continuity- system/data **availability**
  - Network protection
  - Security management process
    - Administrative, Physical, Technical safeguard areas
  - Security incident prevention and mitigation

The HIPAA Security Rule covers all of these requirements, so compliance with it also brings serendipity compliance with other regulations! HITECH, and Omnibus, reiterates/strengthens all of these good business practices and regulatory requirements.

California's Basic Legal Concept for Security

- "a business that owns, licenses, or maintains personal information about a California resident shall implement and maintain ***reasonable security*** procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." – Cal. Civ. Code §1798.81.5(b)
- The 20 controls in the Center for Internet Security's (CIS) Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment ***constitutes a lack of reasonable security.***

Center for Internet Security (CIS) Critical Security Controls…

- CSC 1 Inventory of Authorized and Unauthorized Devices
- CSC 2 Inventory of Authorized and Unauthorized Software
- CSC 3 Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- CSC 4 Continuous Vulnerability Assessment and Remediation
- CSC 5 Controlled Use of Administrative Privileges
- CSC 6 Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7 Email and Web Browser Protection
- CSC 8 Malware Defenses
- CSC 9 Limitation and Control of Network Ports, protocols, and Services
- CSC 10 Data Recovery Capability

Center for Internet Security (CIS) Critical Security Controls

- CSC 11 Secure Configurations for Network Devices (Firewalls, Routers, Switches)
- CSC 12 Boundary Defense
- CSC 13 Data Protection
- CSC 14 Controlled Access Based on the Need to Know
- CSC 15 Wireless Access Control
- CSC 16 Account Monitoring and Control
- CSC 17 Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18 Application Software Security
- CSC 19 Incident Response and Management
- CSC 20 Penetration Tests and Red Team Exercises

For HIPAA/HITECH Security Compliance

need to address:

- Authentication
- Access (Authorized and Unauthorized)
- Logging and Auditing
- Protecting data in storage (locally and remotely)
- Protecting data being transmitted
- Protection from Malware,, etc.
- Physical Security
- Need policies that mirror operating environment
- Identifying and reporting security incidents and breaches
- Training Staff

Two of the most important Security Rule requirements

- Risk Analysis
  - That leads to a Risk Management Plan
- Evaluation
  - That periodically reviews and make a determination if the administrative, physical, and technical requirements are still being met
    - It involves both and administrative (policies, procedures, processes) and a technical review

Risk Analysis vs. Gap Analysis

- "If you know the enemy and know yourself, you need not fear the result of a hundred battles. **(Risk Analysis)**.
- If you know yourself and not the enemy, for every victory gained you will also suffer a defeat." **(Gap Analysis)** — Sun Tzu, *The Art of War*.(circa 500 B.C.)

- **Gap analysis** helps identify the vulnerabilities in your information assets;
- **Risk analysis** examines those vulnerabilities in light of potential threats that can exploit them and their likelihood of occurrence and the resulting impacts.

Risk Analysis / Gap Analysis*

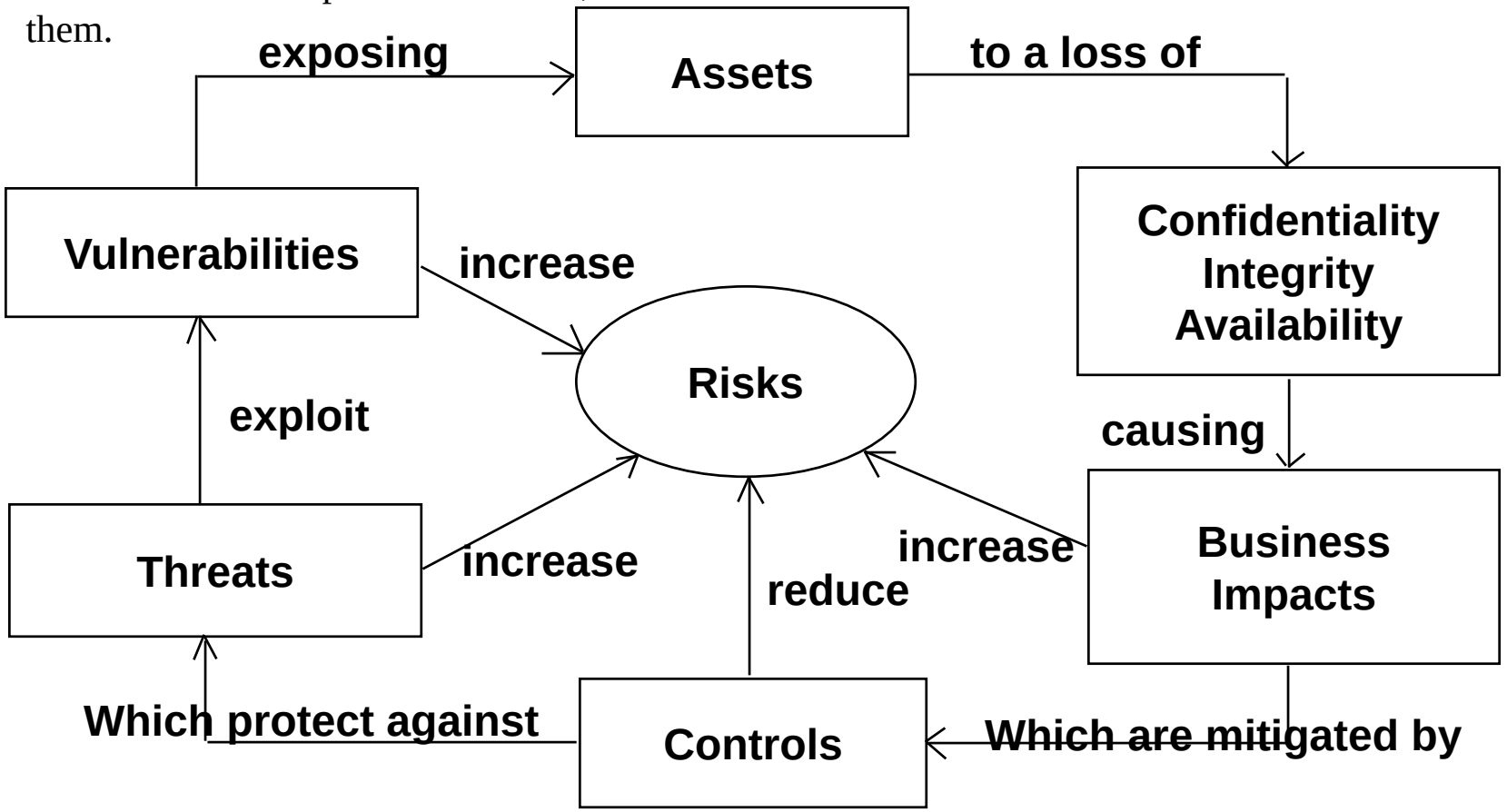
- A **risk analysis** is a necessary tool to assist covered entities and business associates conduct a **comprehensive** evaluation of their **enterprise** to identify the ePHI and the risks and vulnerabilities to the ePHI. It looks at all of the locations of ePHI the corresponding threats to each and the impact A covered entity or business associate may use the results of a risk analysis to make appropriate, enterprise-wide modifications to their ePHI systems to reduce risks to a reasonable and appropriate level.

- A **gap analysis** is typically a narrowed examination of a covered entity or business associate's enterprise to assess whether certain controls or safeguards required by the Security Rule have been implemented. A gap analysis provides a high-level overview of how an entity's safeguards are implemented and show what is incomplete or missing (*i.e.*, spotting "gaps"), but it generally **does not** provide a comprehensive, enterprise-wide view of the security processes of covered entities and business associates. It is also a tool utilized in showing regulatory compliance.

* the OCR definition

Risk Analysis Process

1. Start with identifying assets; then 2. the vulnerabilities of each of the assets; then 3.t he threats that cloud exploit those vulnerabilities; then 4. the results to lost CIA; then 5. what are the business impacts of this loss; then 6. what controls are needed to minimize/eliminate them.



Source: Ken Jaworski, CISSP

Definitions

- **Assets**: for every information system that has ePHI
  - ❖ Hardware: computers, workstations, laptops, pdas, modems, medical equipment, radiology storage devices, etc.
  - ❖ Software: applications, databases, operating systems, encryption; purpose of each process/system
  - ❖ Telecommunications networks: internal and external connectivity, servers, remote access
  - ❖ Users internal and external / Business Associates / Vendors
  - ❖ Facilities: number of locations; physical environment
- **Threat**: The potential for a natural, human, and/or environmental threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability
- **Vulnerability**: A flaw or weakness in a system's security procedures, design, implementation, and/or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- **Controls**:
  - **Preventive controls** inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
  - **Detective controls** warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.
- **Business Impacts: Quantitative (measurable loss =** total risk (annualized loss expectancy = single-loss expectancy x annualized rate of occurrence); **Qualitative** (**relative** – high / medium / low)

Risk Assessment ⇒ Risk Management

- Risk can either be:
  - Mitigated/Reduced (Applying controls)
  - Transferred (Insuring against a loss)
  - Accepted (Doing nothing, but recognizing risk)
- Risk should be handled in a cost-effective manner relative to the value of the asset
- Risk is addressed differently by various organizations
  - Largely dependent on the level of organizational risk tolerance *and*
  - Within what is construed as "reasonable" and "appropriate"

HIPAA/HITECH SECURITY
A Full Set of POLICIES AND PROCEDURES…

For audit purposes, all of these are best arrayed in a "book" that aligns each with the regulatory requirement

- Overview of the Security Rule
- Organizational Requirements
  - Designation of a Security Officer; Designation of a Privacy Officer (could be same person in a small practice)
- Documentation Requirements
- Business Associate Agreements

<u>Administrative Safeguards</u>

- The Security Management Process
  - Risk Analysis
  - Risk Management
  - Sanctions
  - Information System Activity Review
- Workforce Security
  - Authorization and/or Supervision
  - Workforce Clearance
  - Termination Procedure
- Information Access Management
  - Access Authorization
  - Access Establishment and Authorization

HIPAA/HITECH SECURITY
POLICIES AND PROCEDURES…

- Security Awareness and Training
  - Security Reminders
  - Protection from Malicious Software
  - Log-in Monitoring
  - Password Management
- Security Incident Procedures
  - Response and Reporting
- Contingency Plan
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode Operation Plan
  - Testing and Revision
  - Applications and Data Criticality Analysis
- Evaluation

Physical Safeguards

- Facility Access Controls
  - Contingency Operations
  - Facility Security Plan
  - Access Control and Validation Procedures
  - Maintenance Records

HIPAA/HITECH SECURITY
POLICIES AND PROCEDURES

- Workstation Use
- Workstation Security
- Device and Media Controls
  - Disposal
  - Media Reuse
  - Accountability
  - Data Backup and Storage

Technical Safeguards

- Access Control
  - Unique User Identification
  - Emergency Access Procedures
  - Automatic Logoff
  - Encryption and Decryption
- Audit Control
- Integrity
  - Mechanism to Authenticate ePHI
- Person or Entity Authentication
- Transmission Security
  - Integrity Controls
  - Encryption

Additional Resources

- **HIPAA Security Rule Guidance Material**
  https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es
- **Risk Analyses vs. Gap Analyses – What is the difference?**
  https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf

Thank You !

Questions?

John Parmigiani
410-750-2497
jcparmigiani@comcast.net
www.johnparmigiani.com