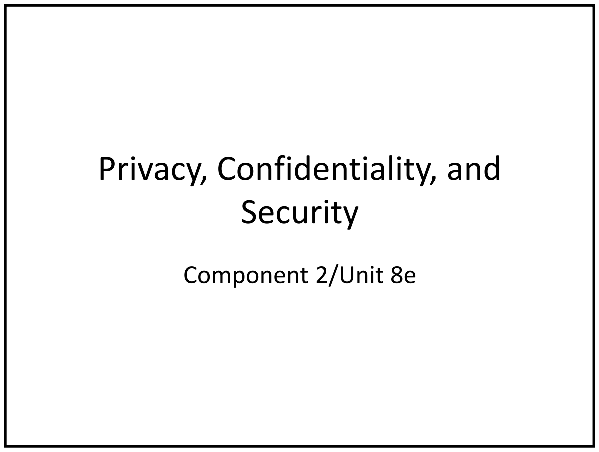
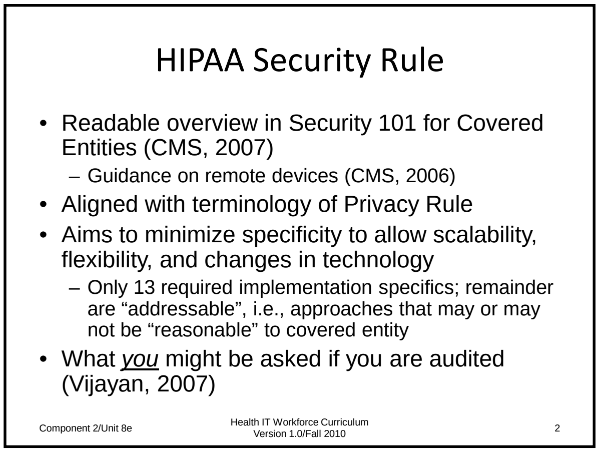


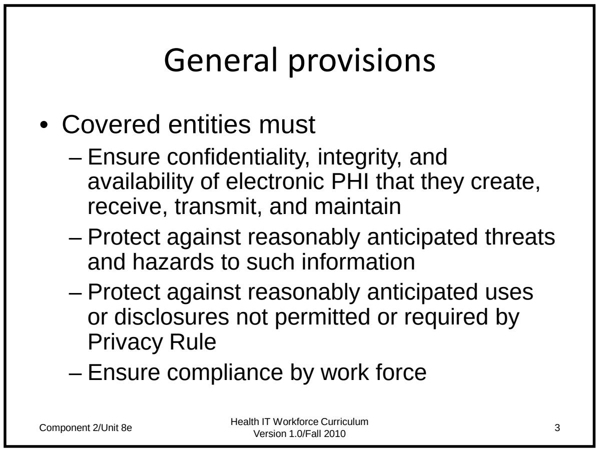
Privacy, Confidentiality, and Security

Component 2/Unit 8e



HIPAA Security Rule

- Readable overview in Security 101 for Covered Entities (CMS, 2007)
  - Guidance on remote devices (CMS, 2006)
- Aligned with terminology of Privacy Rule
- Aims to minimize specificity to allow scalability, flexibility, and changes in technology
  - Only 13 required implementation specifics; remainder are "addressable", i.e., approaches that may or may not be "reasonable" to covered entity
- What *you* might be asked if you are audited (Vijayan, 2007)

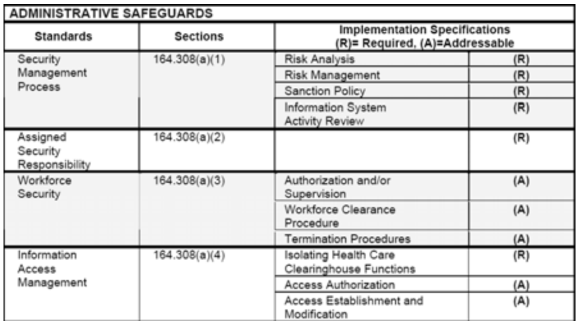


General provisions

- Covered entities must
  - Ensure confidentiality, integrity, and availability of electronic PHI that they create, receive, transmit, and maintain
  - Protect against reasonably anticipated threats and hazards to such information
  - Protect against reasonably anticipated uses or disclosures not permitted or required by Privacy Rule
  - Ensure compliance by work force

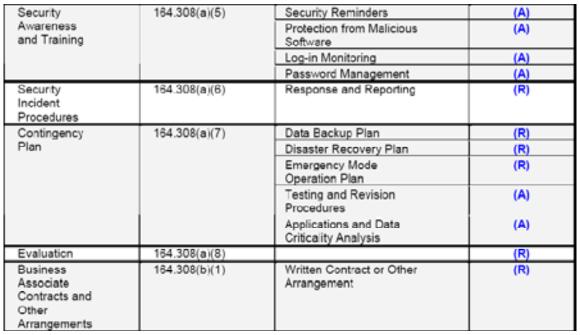
Required safeguards

- Grouped into three categories
  - – Administrative – policies and procedures designed to prevent, detect, contain, and correct security violations
  - – Physical – protecting facilities, equipment, and media
  - – Technical – implementing technological policies and procedures
- Following slides from Security 101

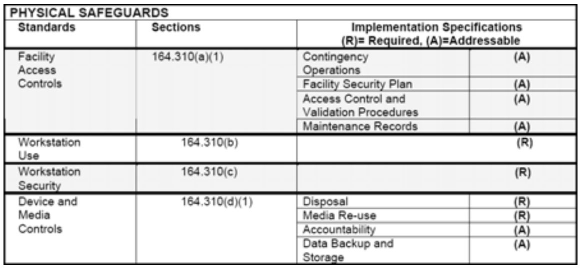


ADMINISTRATIVE SAFEGUARDS

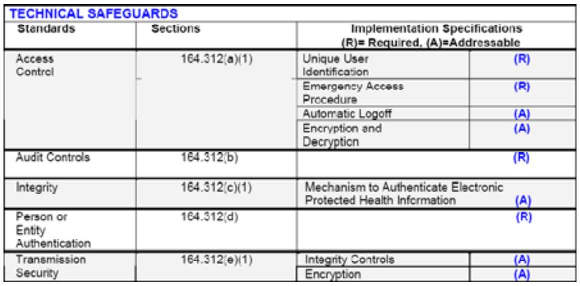
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)



Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	(R)



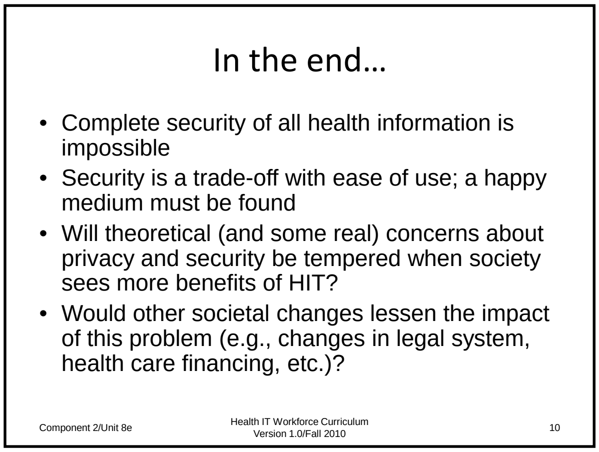
PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)



TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Other regulations

- Business associates are required to
  - Implement safeguards to protect covered entity’s PHI
  - Ensure its agents and subcontractors meet same standards
  - Report to covered entity any security incident
- Documentation of covered entity must
  - Be maintained for six years
  - Available to those responsible for implementing
  - Reviewed and updated periodically
- HITECH meaningful use criteria specify use of various encryption standards, e.g., AES, TLS, IPsec, SHA-1



In the end…

- Complete security of all health information is impossible
- Security is a trade-off with ease of use; a happy medium must be found
- Will theoretical (and some real) concerns about privacy and security be tempered when society sees more benefits of HIT?
- Would other societal changes lessen the impact of this problem (e.g., changes in legal system, health care financing, etc.)?

Component 2/Unit 8e

Health IT Workforce Curriculum
Version 1.0/Fall 2010

10