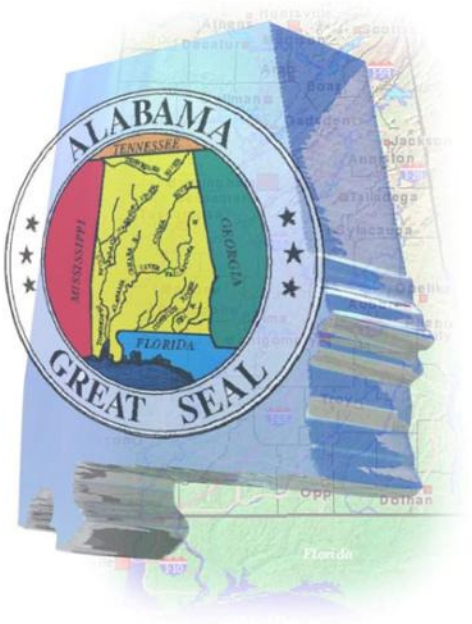
Introduction to HIPAA

Understanding the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

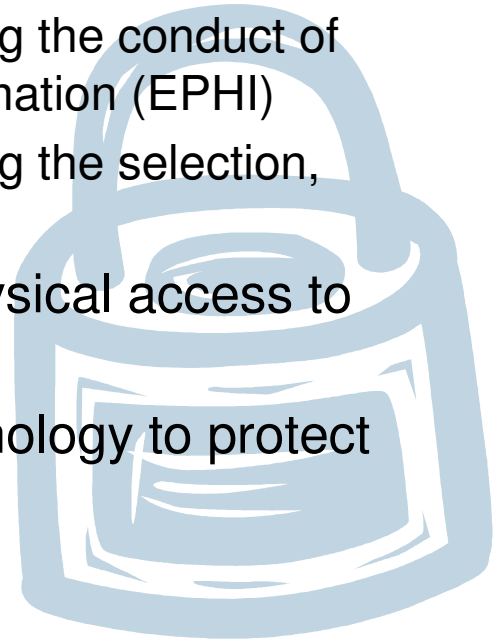


Covered Entities

- The HIPAA Security Rule applies to Health Plans, Healthcare Clearinghouses, and Healthcare Providers
- Health Plans are defined as any individual or group plan that provides or pays for the cost of medical care, which includes:
  - Medicare,
  - Medicaid,
  - Children's Health Programs, and
  - Other programs operated at the state and federal levels.

Safeguards

- HIPAA Security Standards mandate “Safeguards” be taken by covered entities in *Administrative*, *Physical* and *Technical* areas
- *Administrative* Safeguards require:
  - Documented policies and procedures for daily operations
  - Documented policies and procedures for managing the conduct of employees with Electronic Protected Health Information (EPHI)
  - Documented policies and procedures for managing the selection, development, and use of “security controls”
- *Physical* Safeguards concern the control of physical access to EPHI stored on hardware and electronic media
- *Technical* Safeguards specify how to use technology to protect and control EPHI

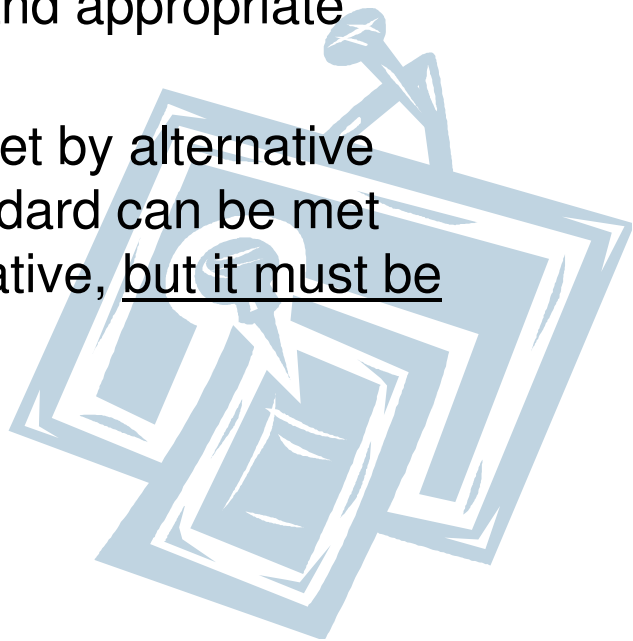


"Standards" vs. "Implementation Specifications"

- Standards explain what a Covered Entity *must do*
- Implementation Specifications explain *how to* do it
- The HIPAA Security Rule requirements include 18 Standards
  - Administration Safeguards has 9 standards
  - Physical Safeguards has 4 standards
  - Technical Safeguards has 5 standards
  - 12 standards have implementation specifications
  - 6 standards have no implementation specifications
- There are a total of 36 Implementation Specifications for these 12 standards
  - 14 Specifications are "Required"
  - 22 Specifications are "Addressable"

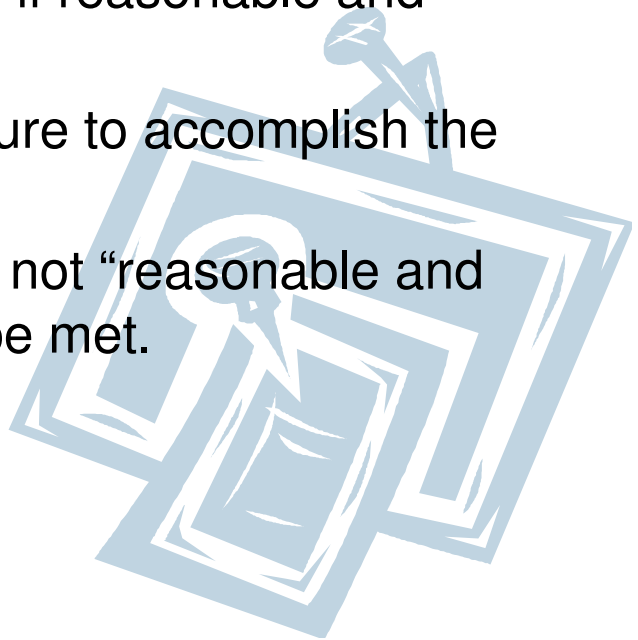
"Addressable vs. "Required"

- "Required" means the covered entity must comply with the standard
- "Addressable" does **not** mean Optional
  - A covered entity must use reasonable and appropriate measures to meet the standard
  - Addressable implementations can be met by alternative means, or an entity can decide the standard can be met without the implementation of an alternative, <u>but it must be documented</u>



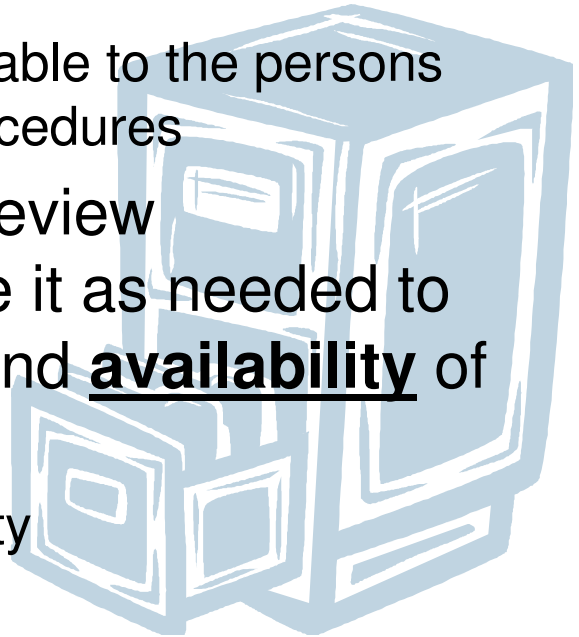
Addressable Options

- The HIPAA Security rule requires covered entities to do one of three things regarding any addressable standard:
  - Implement an addressable specification if reasonable and appropriate, or
  - Implement an alternative security measure to accomplish the purposes of the standard, or
  - Implement nothing if the specification is not “reasonable and appropriate” and the standard can still be met.



Documentation Standards

- Covered entities must maintain all documentation, policies, and procedures required by the Security Rule for 6 years from the date of creation or last day in effect
  - Documentation must also be made available to the persons responsible for implementing related procedures
- Covered entities must periodically review documentation to revise and update it as needed to ensure **confidentiality**, **integrity**, and **availability** of EPHI
  - Bedrock Principles of Information Security



Other "Highlights" from the Security Rule

- The Rule contains no specific technology recommendations
- The Rule defines the "minimum standard" or the least that a covered entity must do to protect EPHI
  - A covered entity may choose to do more
  - Such a decision should be based upon individual risk analysis and vulnerability assessment
- The Rule requires a covered entity to do a thorough and accurate "risk analysis," as well as to document this process
  - Risk analysis is also recognized as being an individual responsibility and the results of each covered entity's analysis will be unique unto itself
  - While the threats to EPHI should be well known, each covered entity's own vulnerability will determine the risk specific to that entity

Other "Highlights" from the Security Rule

- The Rule is based on many different security guidelines, standards and information security industry "best practices"
  - Many of these have been in place for a number of years within the government and certain industries like banking
  - HIPAA mandates these Standards with their requirements and implementation specification upon the healthcare industry
- All covered entity staff, including management, physicians, and those who work at home, must comply with the Security Rule
  - Including telecommuters or others who connect remotely to a covered entity's information system
  - Including physicians who may or may not be employees of a hospital or medical center

Other "Highlights" from the Security Rule

- A covered entity must document Security Rule implementation decisions
  - This is part of the Documentation standards
  - As long as documentation is proper, some implementation decisions later found not complaint with the HIPAA Security rule might incur no penalties on the covered entity
- A covered entity must regularly train employees
  - HIPAA Security training should become part of a covered entity's new employee orientation program, as well as any annual skills demonstration, JCAHO (Joint Commission on the Accreditation of Health Care Organizations) preparation, or other state certification process

Administrative Safeguards

Standards	Implementation Specifications (R)=Required, (A)=Addressable	
Security Management Process	Risk Analysis	(R)
	Risk Management	(R)
	Sanction Policy	(R)
	Information Systems Activity Review	(R)
Assigned Security Responsibility		(R)
Workforce Security	Authorization and/or Supervision	(A)
	Workforce Clearance Procedure	(A)
	Termination Procedures	(A)
Information Access Management	Isolating Healthcare Clearinghouse Function	(R)
	Access Authorization	(A)
	Access Establishment and Modification	(A)

Standards	Implementation Specifications (R)=Required, (A)=Addressable	
Security Awareness and Training	Security Reminders	(A)
	Protection from Malicious Software	(A)
	Login Monitoring	(A)
	Password Management	(A)
Security Incident Procedures	Response and Reporting	(R)
Contingency Plan	Data Backup Plan	(R)
	Disaster Recovery Plan	(R)
	Emergency Mode Operation Plan	(R)
	Testing and Revision Procedure	(A)
	Applications and Data Criticality Analysis	(A)
Evaluation		(R)
Business Associate Contracts and Other Arrangements	Written Contracts or Other Arrangements	(R)

Physical Safeguards

Standards	Implementation Specifications (R)=Required, (A)=Addressable	
Facility Access Controls	Contingency Operations	(A)
	Facility Security Plan	(A)
	Access Controls and Validation Procedures	(A)
	Maintenance Records	(A)
Workstation Use		(R)
Workstation Security		(R)
Device and Media Controls	Disposal	(R)
	Media Reuse	(R)
	Accountability	(A)
	Data Backup and Storage	(A)

Technical Safeguards

Standards	Implementation Specifications (R)=Required, (A)=Addressable	
Access Controls	Unique User Identification	(R)
	Emergency Access Procedure	(R)
	Automatic Logoff	(A)
	Encryption and Decryption	(A)
Audit Controls		(R)
Integrity	Mechanism to Authenticate EPHI	(A)
Person or Entity Authentication		(R)
Transmission Security	Integrity Controls	(A)
	Encryption	(A)

Steps for Complying with the Security Rule

- Assess current security, risks, and gaps
- Develop an implementation plan
  - Review the Security Rule standards and specifications
  - Review addressable implementation specifications
  - Determine security measures
- Implement solutions
- Document decisions
- Reassess periodically

New/Future Requirements

- The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act (ARRA) of 2009, imposes new privacy and security requirements
  - Business associates of covered entities must comply with HIPAA Security Rule safeguard standards beginning February 17, 2010
  - Entities that provide data transmission of PHI to covered entities or their business associates must enter into a written agreement with the covered entity containing the same requirements applicable to business associates
  - New breach notification rules apply to covered entities and business associates