



# HIPAA-

## How the Security Rules Will Impact Employers and the Health Plans They Sponsor

---

Jessica Bernanke  
Ken Duarte  
Georgina O'Hara

December 15, 2004

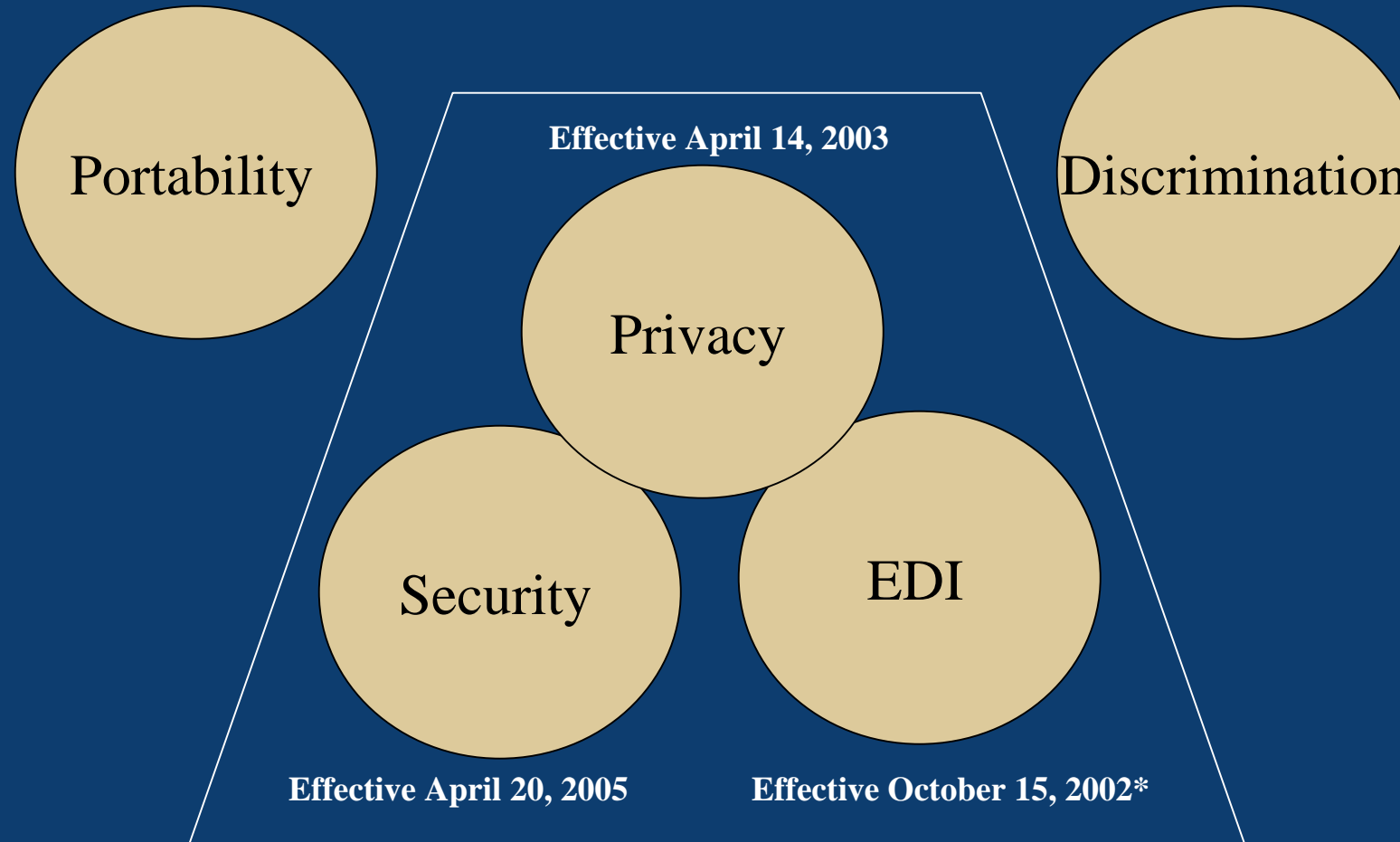
---

Morgan, Lewis & Bockius LLP

## Purpose of Security Rules

- To adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.
- No standard measures currently exist in the health care industry that address all aspects of the security of electronic protected health information while it is being stored or during the exchange of that information between entities.

# HIPAA's Scope



# Overlap Between Privacy and Security Rules

- **Cover the Same Entities** (“Covered Entities”)
  - Health Care Clearinghouse.
  - Health Care Provider who transmits health information.
  - Health Plan (including HMO or other health insurance issuer).
- **Scalable Standards**
  - Each covered entity should comply in a manner that makes operational sense for it.
  - Size, complexity, technical infrastructure, costs, risks and capabilities of covered entity should be taken into account.
  - The Security Standards are technology-neutral.

## PHI v. ePHI

- A crucial distinction between the Privacy Rule and the Security Rule is the type of information covered by the Rule.
  - Privacy Rule covers PHI - Information created or received by a covered entity that relates to past, present, or future physical or mental health or condition; provision of health care; or payment for provision of health care, and that identifies an individual or could be used to identify an individual. This covers information in any format or medium - paper, oral or electronic.
  - Security Rule covers ONLY ePHI - PHI in electronic media or format at rest or in transmission.

## Examples of ePHI (and not ePHI)

- Examples of ePHI:
  - magnetic tape
  - disk or optical disk
  - computerized information
  - internet transmission
  - network information
  - telephone response and “fax back” (a request for information from a computer made via voice or telephone keypad input with the requested information returned as a fax)
- Examples of NOT ePHI:
  - copy machines
  - paper files
  - “paper to paper” faxes
  - person-to-person telephone calls
  - video teleconferencing
  - voicemail messages

# Compliance Scheme

- The Security Rule sets out defined Standards, which must be met, which are generally grouped into 3 categories:
  - **Administrative.** Administrative actions, and policies and procedures that relate to the “selection, development, implementation and maintenance of security measures to protect ePHI” and the management of employees with regard to protecting ePHI.
  - **Physical.** Physical measures to protect the “electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.”
  - **Technical.** The technology that protects ePHI and controls access to it.

## Required v. Addressable

- The Standards include Implementation Specifications that are either required or addressable.
  - If a specification is required, the covered entity must implement it.
  - If a specification is addressable, the covered entity has to determine whether it is a “reasonable and appropriate” safeguard. And if it is, the covered entity must implement it.

## Required v. Addressable (continued)

- If the covered entity finds that implementing the specification is not reasonable and appropriate, it must:
  - document why it would not be reasonable and appropriate; and
  - implement an equivalent/alternative measure that is reasonable and appropriate, and document why that measure is appropriate and how that measure meets the Standard, or
  - take no action with regard to the specification, and document why no action was taken and how the Standard is being met.

# Security Rule Documentation Requirements

- **Plan Amendments.** Plan Documents must be amended again.
  - These amendments will provide that the plan sponsor will reasonably and appropriately safeguard ePHI created received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
- **Business Associate Agreements.** Must be amended to include Security language (detailed later).
- **Policies and Procedures.** Should be designed to comply with the security rules and should be:
  - Reasonable.
  - Tailored to the amount of ePHI used or held by the health plan.
  - Flexible.

# Penalties

- **Civil**
  - \$100 per violation, up to
  - \$25,000 per year per violation.
- **Criminal** (knowing misuse)
  - Up to \$50,000 and 1 year imprisonment.
  - Increased penalties for false pretenses or intent to sell.
- **Office of Civil Rights** has enforcement authority
  - Regulations forthcoming.

# Administrative Standards and Implementation Specifications

- There are 9 Administrative Standards.
- **1. Security Management Process Standard.**  
Implement policies and procedures to prevent, detect, contain and correct security violations.
  - Risk Analysis (Required Implementation Specification ("RIS")).  
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI that your employer/plan sponsor maintains, transmits or receives.

# Security Management Process Standard - Risk Analysis RIS

- **Risk Analysis Steps:**
  - Locate/Map the ePHI that is stored, transmitted or received at your employer/plan sponsor.
  - Review Current Electronic Security Measures (written and unwritten).
  - Identify Possible Risks/Threats to Information/Computer Systems that Store or Transmit ePHI.
  - Address the Addressable Implementation Specifications.

# Security Management Process Standard - Risk Management RIS

- **Risk Management (RIS).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to ensure the confidentiality, integrity and availability of ePHI, and to protect against unauthorized access and improper uses and disclosures of ePHI.
  - Review the Risk Analysis to identify any gaps in your administrative, physical and technical safeguards.
  - Remedy any gaps in your security measures.
  - Implement the Standards, RIS, and the reasonable and appropriate AIS and/or alternative measures.

# Security Management Process Standard -Sanction and Info. System Review RIS

- **Sanction Policy (RIS).** Implement and apply appropriate sanctions against workforce members who fail to comply with your Security Rule policies and procedures.
- **Information System Activity Review (RIS).** Implement policies and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

# Assigned Security Responsibility Standard

- **2. Appoint a Security Official (RIS).** The Security Official is responsible for the development and implementation of the Security Rule policies and procedures.
  - Individual accountable for compliance with the Security Rule.
  - Responsible for the management and supervision of (1) the use of security measures to protect data, and (2) the conduct of the personnel who have access to ePHI.
  - Person should have technology knowledge, and know and understand the rules and regulations.
  - Privacy Officer and Security Official can be the same person.

# Security Awareness and Training Standard

- **3. Security Awareness and Training Standard.** Implement a security awareness training program for all workforce members (including management) as is reasonable and appropriate for those individuals to carry out their job functions.
  - Current employees must be trained by 4/20/2005.
  - New employees must be trained within a reasonable time after gaining access.
  - If policies materially change, affected employees must be trained within a reasonable time.
  - Training must be documented and maintained for 6 years.

## Security Awareness and Training Standard (con't)

- In addition to the training requirement, this Standard includes the following Addressable Implementation Specifications:
  - Security Reminders (AIS).
  - Protection from Malicious Software (AIS).
  - Log-In Monitoring (AIS).
  - Password Management (AIS).

# Business Associate Agreements Standard

- **4. Business Associate Agreement Standard (RIS).** By April 20, 2005, the Business Associate Agreements need to be amended to require business associates to:
  - Implement administrative, physical, and technical safeguards that reasonably and appropriately safeguard the confidentiality, integrity, and availability of the ePHI that it creates, maintains, or transmits on behalf of the covered entity;
  - Ensure that any agent, including a subcontractor, to whom it provides ePHI agrees to implement reasonable and appropriate safeguards to protect that information; and
  - Report to the plan any security incident of which it becomes aware.
  - The BAA also must provide for termination of the BAA if there is a material breach.

# Additional Administrative Safeguards

- **5. Workforce Security Standard.** Implement policies and procedures to ensure that all workforce members have necessary access to ePHI, and that unauthorized workforce members do not have access to ePHI.
  - Authorization and/or Supervision (AIS).
  - Workforce Clearance Procedures (AIS).
  - Termination Procedures (AIS).
- **6. Information Access Management.** Implement policies and procedures for authorizing access to ePHI that are consistent with the Privacy Rule requirements.
  - Access Authorization (AIS).
  - Access Establishment and Modification (AIS).

## Additional Administrative Safeguards (con't)

- **7. Security Incident Procedures Standard.** Implement policies and procedures to address “security incidents.” A “security incident” is “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.”
  - Response and Reporting (RIS).

## Additional Administrative Safeguards (con't)

- **8. Contingency Plan Standard.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (fire, vandalism, system failure, etc.) that damages systems that contain ePHI.
  - Data Backup Plan (RIS).
  - Disaster Recovery Plan (RIS).
  - Emergency Mode Operation Plan (RIS).
  - Testing and Revision Procedures (AIS).
  - Applications and Data Criticality Analysis (AIS).
- **9. Evaluation Standard.** Perform periodic technical and non-technical evaluations.

# Physical Standards and Implementation Specifications

- There are 4 Physical Safeguard Standards.
- **1. Facility Access Controls Standard.** Implement policies and procedures to limit physical access to areas and facilities where ePHI is housed, while allowing access to authorized individuals.
  - Contingency Operations (AIS).
  - Facility Security Plan (AIS).
  - Access Control and Validation Procedures (AIS).
  - Maintenance Records (AIS).

# Physical Standards and Implementation Specifications (continued)

- **2. Workstation Use Standard (RIS).** Implement procedures that specify the proper function to be performed, the manner in which those functions are to be performed, the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.
- **3. Workstation Security Standard (RIS).** Implement physical security safeguards for all workstations that access ePHI in order to restrict access to authorized users.

# Physical Standards and Implementation Specifications (continued)

- **4. Device and Media Controls Standard.** Implement procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within a facility.
  - Disposal (RIS).
  - Media Re-Use (RIS).
  - Accountability (AIS).
  - Data Back-Up Storage (AIS).

# Technical Standards and Implementation Specifications

- There are 5 Technical Standards.
- **1. Access Controls Standard.** Implement technical policies and procedures so that access to ePHI maintained on electronic information systems is only available to those persons or software programs that have been granted access rights.
  - Unique User Identification (RIS).
  - Emergency Access Procedure (RIS).
  - Automatic Logoff (AIS).
  - Encryption and Decryption (AIS).

## Technical Standards and Implementation Specifications (continued)

- **2. Audit Controls Standard (RIS).** Implement hardware, software, and procedures and mechanisms that record and examine activity in information systems that contain or use ePHI.
- **3. Integrity Standard (RIS).** Implement procedures to protect ePHI from improper alteration or destruction.
- **4. Person or Entity Authentication (RIS).** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

## Technical Standards and Implementation Specifications (continued)

- **5. Transmission Security Standard.** Implement technical policies and procedures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.
  - Integrity Controls (AIS).
  - Encryption (AIS).

## Steps Towards Compliance

- **STEP 1** - Designate a Team (including IT, HR and Legal), and Appoint a Security Official.
- **STEP 2** - Conduct the Risk Analysis Audit (including, address the Addressable Specifications).
- **STEP 3** - Implement Standards and Implementation Specifications and remedy any gaps in security measures.

## Steps Towards Compliance

- **STEP 4** - Develop, implement and document the policies and procedures related to the Security Rule.
- **STEP 5** - Amend the plan document to include Security Rule provisions, and ensure that the business associate agreements include Security Rule provisions.
- **STEP 6** - Conduct Workforce Training.

## CONTACT INFORMATION

- **Jessica Bernanke** (Washington, DC Office)
  - 202.739.5447; [jbernanke@morganlewis.com](mailto:jbernanke@morganlewis.com)
- **Ken Duarte** (Dallas, TX Office)
  - 214.438.1554; [kduarte@morganlewis.com](mailto:kduarte@morganlewis.com)
- **Georgina O'Hara** (Philadelphia, PA Office)
  - 215.963.5188; [go'hara@morganlewis.com](mailto:go'hara@morganlewis.com)