Plan Year IEBP Staff Education Resource Library

HIPAA Privacy, Breach Notification & Security Training

Champion the Integrity of the Healthcare Dollar by Optimized Efficient Performance Based Outcome | Dedicated to Service | Engage in the Process | Embrace in Proactive Opportunities for Improvement | Execute with Excellence | Political Subdivision Value Based Synergy Managing the Multi-Faceted Solutions to Healthcare Costs and Performance Based Outcome | 24/7/365
Privacy Rule

› Compliance & Enforcement

- Who is responsible for enforcing the Privacy, Breach Notification & Security Rules?
- Potential Criminal Penalties for Noncompliance
- Potential Civil Penalties for Noncompliance
Privacy Rule

➢ Who is a “Covered Entity”?  
➢ What is “Protected Health Information”?  
➢ What is a “Hybrid Entity”?  
➢ Who are “Business Associates”?  
➢ What types of media are subject to the Privacy Rule?
Privacy Rule

- Required Disclosures of Protected Health Information
- Permitted Uses and Disclosures of Protected Health Information
  - Treatment
  - Payment
  - Health Care Operations
- Minimum Necessary Standard
Privacy Rule

- Notice of Privacy Practices
  - Required Content
  - Providing Notice to Employees
  - Posting on Website
Privacy Rule

› Authorizations

▪ Unless a use or disclosure of Protected Health Information is specifically permitted by the Privacy Rules, a written, signed authorization is required from the individual

▪ The rules for a valid authorization include:
  • Required core elements
  • Required statements
Privacy Rule

Individual Rights under the Privacy Rule

- Right to Request Additional Protections
  - Additional Restrictions
  - Confidential Communications
- Right to Access Protected Health Information
- Right to Amend Protected Health Information
- Right to Receive an Accounting of Disclosures
Privacy Rule

- Administrative Responsibilities
  - Personnel Designations
  - Training Workforce
  - Safeguarding Protected Health Information
  - Privacy Complaints
  - Sanctioning Workforce
  - Mitigation of Harm
  - Refraining from Intimidating or Retaliatory Acts
  - Waiver of Rights
  - Policies and Procedures
  - Documentation
Breach Notification Rule

- What is a “breach” of Protected Health Information
- Covered Entities must have a process for investigating possible breaches of an individual’s Protected Health Information
- Notification requirements in the event of a breach
Security Rule

- The Security Rule applies to Electronic Protected Health Information (ePHI) that a Covered Entity creates, receives, maintains, or transmits.
- A Covered Entity must ensure the Confidentiality, Integrity, and Availability of Electronic Protected Health Information.
Security Rule

Requirements of the Security Rule are scalable and flexible. A Covered Entity’s compliance plan may take into account its:

- Size
- Complexity
- Capabilities
- Technical Infrastructure
- Cost of Security Measures
- Potential Security Risks
Security Rule

- The Security Rule is organized into Standards
  - A Covered Entity must meet each Standard
- Each Standard may have one or more Implementation Specifications
  - Implementation Specifications may be required or addressable
The Security Rule is separated into:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
Security Rule

- Administrative Safeguards are administrative actions, policies and procedures that:
  - Manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information
  - Manage the conduct of employees in protecting Electronic Protected Health Information
Physical Safeguards are physical policies and procedures to protect records, information systems, and related buildings and equipment from natural and environmental hazards and from unauthorized intrusion.
Security Rule

- Technical Safeguards are the technology and policies and procedures for its use that protect Electronic Protected Health Information.
Have a Great Day!

Your Time is Appreciated