O'HAGAN MEYER

RAPID RESPONSE & INCIDENT MANAGEMENT

Protecting Personal Health Information Under HIPAA

This guide applies to covered entities and their business associates that maintain personal health information (PHI) in any form.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

1. 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
2. Relates to the past, present, or future physical or mental health 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.

HIPAA's Privacy Rule requires the following:

- **Personnel Designations**
  - Each covered entity must designate a privacy official.
  - Each covered entity must designate a contact person or office.
- **Training**
  - The covered entity must train members of its workforce on policies and procedures with respect to PHI, as necessary for those members to carry out their job functions.
- **Safeguards**
  - A covered entity must have in place appropriate administrative, technical and physical safeguards to protect PHI from intentional or unintentional use or disclosure.
- **Complaints**
  - A covered entity must have a process for individuals to make complaints concerning the covered entity's policies and procedures and must document all complaints received and their disposition.
- **Sanctions**
  - A covered entity must have and apply appropriate sanctions against its workers who fail to comply with its policies and procedures and must document any sanctions that are applied.
- **Mitigation**
  - A covered entity must mitigate any harmful effects due to the use or disclosure of PHI in violation of its policies and procedures.
- **Refrain from Intimidating or Retaliatory Acts**
  - A covered entity must refrain from any intimidating or retaliatory acts against any individual for exercising their rights.
- **Waiver of Rights**
  - A covered entity may not require individuals to waive their rights.

- **Policies and Procedures**
  - A covered entity must implement policies and procedures with respect to PHI that are designed to comply with the standards and implementation specifications established under HIPAA.
- **Changes to Policies and Procedures**
  - A covered entity has an obligation to change its policies and procedures to comply with changes in the law.
- **Documentation**
  - A covered entity must maintain the required policies and procedures in written or electronic form and must retain those policies and procedures for a period of six years.

HIPAA's Security Rule applies to covered entities in possession of PHI in electronic form (ePHI) and requires that each covered entity:

- Ensure the confidentiality, integrity, and availability of all ePHI that the covered entity or business associate creates, receives, transmits or stores.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- Ensure compliance by its workforce with the Security Rule.

The Security Rule allows flexibility in how covered entities and their business associates use security measures to comply the required standards and specifications. Covered entities and their business associates should take into account:

- Their size, complexity and capabilities.
- The technical infrastructure, hardware and software security capabilities
- The costs of security measures.
- The probability and criticality of potential risks to ePHI.

The Security Rule sets forth standards for the protection of ePHI. Implementation specifications for these standards are either "required" or "addressable".

- **Required:** A covered entity or business associate must implement the implementation specifications.
- **Addressable:** A covered entity or business associate must do the following:
  1. Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, and then
  2. Implement the implementation specification if reasonable and appropriate, or document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate.

Standards for the Protection of ePHI

- **Administrative Safeguards**
  - Security Management Process
    - Risk Analysis (Required)
    - Risk Management (Required)
    - Sanction Policy (Required)
    - Information System Activity Review (Required)
  - Assigned Security Responsibility
  - Workforce Security
    - Authorization and/or supervision (Addressable)
    - Workforce clearance procedure (Addressable)
    - Termination procedures (Addressable)
  - Information Access Management
    - Isolating Healthcare clearinghouse functions (Required)
    - Access authorization (Addressable)
    - Access establishment and modification (Addressable)
  - Security Awareness and Training
    - ISecurity reminders (Addressable)
    - IProtection from malicious software (Addressable)
    - ILog-in monitoring (Addressable)
    - IPassword management (Addressable)
  - Security Incident Procedures
    - Response and reporting (Required)
  - Contingency Plan
    - Data backup plan (Required)
    - Disaster recovery plan (Required)
    - Emergency mode operation plan (Required)
    - Testing and revision procedures (Addressable)
    - Applications and data criticality analysis (Addressable)
  - Evaluation
  - Proper Business Associate Agreements
- **Physical Safeguards**
  - Facility Access Controls
    - Contingency operations (Addressable)
    - Facility security plan (Addressable)
    - Access control and validation procedures (Addressable)
    - Maintenance records (Addressable)
  - Workstation Use
  - Workstation Security
  - Device and Media Controls
    - Disposal (Required)
    - Media re-use (Required)
    - Accountability (Addressable)
    - Data backup and storage (Addressable)

- **Technical Safeguards**
  - Access Control
    - Unique user ID (Required)
    - Emergency access procedure (Required)
    - Automatic logoff (Addressable)
    - Encryption and decryption (Addressable)
  - Audit Controls
  - Integrity
    - Mechanism to authenticate electronic protected health information (Addressable)
  - Person or Entity Authentication
  - Transmission Security
    - Integrity controls (Addressable)
    - Encryption (Addressable)

- **Organizational Requirements**
  - Business Associate Contracts or Other Arrangements
    - Business Associate contracts (Required)
  - Requirements for group health plans
    - Plant documents must include necessary provisions (Required)

- **Policies and Procedures and Document Requirements**
  - Policies and Procedures
  - Documentation

O'HAGAN MEYER
ATTORNEYS ▲ ADVISORS