

DRAFT

Information Needed for Informed Decision Making Phase I of Security Implementation Methodology

Principles

The following is a list of possible principles that can serve as a foundation for a Security Implementation Methodology. Each organization is encouraged to establish its own set of principles, the list below is illustrative.

1. **Accountability:** Policy and procedures will be defined so that one person (not a committee) is responsible for each aspect of security.
2. **Environment:** Records containing individual health information that makes an individual identifiable shall be created, stored, maintained, used, transmitted, collected, and disseminated in a secure environment. A secure environment is one that promotes confidentiality and integrity without compromising information availability.
3. **Identity:** Every patient, member of the workforce, provider, health plan, and employer will have one, and only one, unique identifier.
4. **Access Control:** Records may be view, entered, changed, or manipulated only by persons within the workforce that are authenticated and are authorized to perform specific operations on the information for specific purposes.
5. **Integrity:** Records will be accurately maintained until properly authorized by policy to be destroyed.
6. **Availability:** Records will be available for timely access by the workforce. Timeliness will be determined primarily by the purpose of the access and the minimum necessary for use and disclosure.
7. **Monitoring and Response:** Active monitoring (detection) of security breaches will be implemented and appropriate actions taken against offenders.

Threats

Threats, in this context, are primarily activities, whether accidental or on purpose, that are associated with unauthorized access to protected health information for whatever purpose. Think of threats as attacks to secure protected information or to make it unavailable for the workforce to use or to destroy the information as it moves from place to place and is used.

There are many people who are threats to protected health information:

- Business Associates (those performing functions for the covered entity involving use and disclosure of individually identifiable health information.
- Trading Partners
- Vendors
- Workforce (insiders)
- Outsiders (including lawyers, those that claim to represent individuals, etc.)
- Hackers

Events or conditions are threats to protected health information include:

- Storms
- Fire
- Floods
- Lack of power
- Explosion
- Business failure
- Inadequate software configuration and version management
- Software that is not secure (allows unauthorized access)
- Software failure
- Hardware that is not secure (allows unauthorized access)
- Hardware failure

Information has a lifecycle. It is originated, queried, modified, and destroyed. Security must be in effect during the entire lifecycle. Some of the most significant threats to data are when it is on its way toward destruction.

Table 1 provides a starting point for identifying security threats within an organization. A partial list of specific threats is categorized by (1) exposure to PHI, (2) unavailability of PHI, (3) malicious intent. Malicious intent is broken out separately because there are specific countermeasures that are necessary to protect against this threat.

Table 1. Security Threats within an Organization

Actors/Events/Conditions	General Threats
Business Associates	<ul style="list-style-type: none"> • Use PHI for purposes other than treatment, payment, and healthcare operations
Trading Partners	<ul style="list-style-type: none"> • Accidental or purposeful disclosure of PHI • Use PHI for purposes other than treatment, payment, and healthcare operations
Vendors Workforce	<ul style="list-style-type: none"> • Accidental or purposeful disclosure of PHI • Employees of vendor use or disclosure of PHI • Workforce use or disclosure of PHI <ul style="list-style-type: none"> -unauthorized access including accidental access -authorized access -accidentally
Outsiders (that are not Business Associates, Trading Partners, or Vendors)	<ul style="list-style-type: none"> • Malicious altering of data (data integrity) • Request of PHI • Unauthorized access • Accidental disclosure
Hackers (breaking in electronically)	<ul style="list-style-type: none"> • Unauthorized access • Unavailability of Information • Malicious altering of data (data integrity) • Unavailability of information
Storms, fire, floods, lack of power, explosion Business sale or failure S/W configuration and versioning	<ul style="list-style-type: none"> • Transfer of PHI upon sale or failure of business • Enables electronic break-ins <ul style="list-style-type: none"> -unauthorized access -unavailability of information -malicious altering of data

Unsecure software	<ul style="list-style-type: none"> • Enables electronic break-ins <ul style="list-style-type: none"> -unauthorized access -unavailability of information -malicious altering of data
Software failure	<ul style="list-style-type: none"> • Enables electronic break-ins <ul style="list-style-type: none"> -unauthorized access -unavailability of information -malicious altering of data
Unsecure hardware	<ul style="list-style-type: none"> • Enables electronic break-ins <ul style="list-style-type: none"> -unauthorized access -unavailability of information -malicious altering of data
Hardware failure	<ul style="list-style-type: none"> • Enables electronic break-ins <ul style="list-style-type: none"> -unauthorized access -unavailability of information -malicious altering of data

Exposure to PHI

- Misdirected faxes
- Misdirected e-mails
- Misdirected mail (internal as well as external)
- Overheard conversations
- Whiteboards, bulletin boards, and the like using for scheduling and other purposes
- Computer screens that are in plain view
- PHI on desks in plain view
- Directories
- Unlocked rooms and filing cabinets
- Files and databases on personal computers
- Files and databases on servers
- Workstations taken off premise
- Remote access to computer systems
- Unauthorized physical and electronic access
- Mistaken identity
- Paper not disposed of properly
- Workstations and storage media not disposed of properly

Unavailable PHI

- Lost PHI
- Stolen PHI
- Accidental or purposeful alteration of Phi
- Disaster
- Denial of service attacks

Malicious Intent

- Past member of the workforce
- Current member of the workforce
- Outsiders unrelated to the current of past workforce

Countermeasures consist of formal measures implemented by the organization to control and monitor access. A list of possible countermeasures includes:

- Effective policy and procedures followed by the workforce
- Business Associate Agreements
- Trading Partner Agreements
- Documentation of events (primarily for two purposes: (1) better detection of a security breach, and (2) analysis of damage for damage control and improved processes)
- Employee handbook
- Workforce training
- Virus checking
- Technical services mechanisms (firewalls, SSL, encryption, digital certificates, single sign-on, VPNs, passwords, intrusion detection, system configuration, screen savers, etc.)
- Physical mechanisms (locks, security tokens, badge readers, etc.).
- Software (operating system, system level functions, infrastructure, applications, communications protocols, etc.) that restricts access.

Infrastructure Identification

To reduce the cost of implementing security and to assure the consistent application of certain policies and procedures across the organization, security infrastructure may be needed. Infrastructure supports security policy and procedures and cuts across organizational boundaries and includes information technology.

One form of infrastructure is to centralize various functions. Centralize, in this context, implies one or more locations or places, not just one location or place. The larger the organization, the more locations will be involved.

It is important to decide on the functions that need to be centralized to achieve the infrastructure goals. A list of specific infrastructure goals may include:

- Naming a security officer with the scope of being the entire organization
- Security policy and procedures approval process
- Business associate agreements
- Trading partner agreements
- Password or certificate control
- Single sign-on
- Single identifier for identity
- File of approved access controls (manual or electronic) by name
- Access controls across all electronic systems per the file of approved access controls
- Implementation of a security monitoring system

The larger the organization, the more the infrastructure needs to be supported by computer technology.

Decision Making Phase II of Security Implementation Methodology

To carry out the second phase of the security implementation methodology, an organization must decide what to do and prioritize the projects and tasks according to funds, resources, and time available.

As is the case with privacy implementation, organization will not have the resources to implement everything at once. The following list can be a starting point to establish project priorities.

1. Name a security officer (this is not required by HIPAA but clearly was intended, and it is a good idea).
2. Establish a base line and plan of execution
3. Implement restrictions to data (physical and electronic).
4. Implement identity systems
5. Establish procedures for obtaining authorization (access to information).
6. Establish access controls.
7. Implement software configuration and version management
8. Train the workforce
9. Monitor security compliance
10. Implement disaster planning