HIPAA

BASIC ELEMENTS FOR COMPLIANCE WITH THE SECURITY REGULATIONS

CHECKLISTS

Perform a Risk Analysis

DEVELOPING YOUR HIPAA DOCUMENTS

Pointers for Drafting Policies & Procedures

MASSACHUSETTS MEDICAL SOCIETY

MASSACHUSETTS
MEDICAL SOCIETY

PREPARED FOR THE MASSACHUSETTS MEDICAL SOCIETY
DEPARTMENT OF HEALTH POLICY/HEALTH SYSTEMS
BY SUSAN A. MILLER, JD

Table of Contents

I. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) passed by Congress in 1996 is a comprehensive law that addresses a number of health care issues including data transmission and protection, fraud and abuse, and insurance portability. Subtitle F to HIPAA entitled, "Administrative Simplification," contains provisions governing the transmission and protection of health data and addresses the confidentiality challenges created by the complexity and speed of new technologies used for gathering, storing, and disseminating health data.

The standards established by the federal government under the Administrative Simplification title are intended to promote two goals: (1) uniformity of electronic data interchange and (2) confidentiality of electronic health data. The components of HIPAA Administrative Simplification include the following:

1. Electronic Transactions and Code Sets;
2. Privacy Standards;
3. Security Standards;
4. Unique Identifiers;
5. Electronic Digital Signature; and
6. Enforcement.

Compliance with the Administrative Simplification portion of HIPAA will require significant changes to a physician's medical practice. *Maintaining the confidentiality of patient information, both electronic and written, is a critical aspect of patient care.* The Massachusetts Medical Society has developed this resource guide to assist physicians in complying with the HIPAA Security Standards by the **April 20, 2005** deadline.

This booklet contains practical tools and resources to prepare physicians in solo, small, or mid-sized practices for implementation of the security standards. The following items are included in these materials:

- A checklist to assess and begin your HIPAA security compliance efforts; and
- A checklist to assess your HIPAA security policies and procedures.

II. HIPAA Security Introduction

The HIPAA security standards are found in Part C of 45 Code of Federal Regulations (CFR) Part 164. The security rule focuses on three principles:

- The standards are comprehensive and coordinated to address all aspects of security;
- The standards are scalable so all covered entities of all sizes and types will be able to implement them; and
- The standards are technology neutral. This is necessary to adopt new technologies as they are developed and become generally available.

The final security rule sets out a series of general standards in 45 CFR 164.306, followed by more specific safeguards and standards for administrative, physical, and technical security.

Most of the security standards have accompanying implementation specifications. The specifications describe the action a covered entity must take to comply with the requirement.

A covered entity must comply with all of the security rule's standards, but individual compliance is based on a number of business factors. The Department of Health and Human Services (DHHS) has provided flexibility for implementation to accommodate the differences in covered entities. The general rule found in the HIPAA security regulation at 45 CFR 164.306(b) states that a covered entity "may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications."

The regulatory language in 45 CFR 164.306(b) outlines the general security standard. A covered entity must take into account the following as it plans for, implements, and monitors the HIPAA security standards:

- Its size, complexity, and capabilities;
- Its technical infrastructure, hardware, and software security capabilities;
- The cost of security measures; and
- The probability and criticality of potential risks to electronic protected health information (ePHI).

Number 4 concerns the likelihood that security risks will occur and the seriousness of their impact on the ePHI and business operations.

The Security Standards General Requirements

45 CFR 164.306(a) outlines the four overall compliance requirements for a covered entity as follows:

1. Ensure confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy part of the HIPAA regulations; and
4. Ensure compliance with the security subpart of the HIPAA regulations by a covered entity's workforce.

45 CFR 164.304 defines confidentiality, integrity, and availability as:

Confidentiality:	Data or information is not made available or disclosed to unauthorized persons or processes.
Integrity:	Data or information have not been altered or destroyed in an unauthorized manner.
Availability:	Data or information is accessible or usable upon demand by an authorized person.

These four general requirements are important because DHHS views these requirements as the acceptable level of risk for security compliance. The only threats and hazards that are exceptions are those that cannot be "reasonably anticipated." The requirements state that an entity needs to "protect against any" and "ensure… all." "Any" and "all" are *absolutes*. "Ensure" is a very high legal standard.

There are three major sections to the security safeguards in the HIPAA security rule:

1. Administrative Safeguards;
2. Physical Safeguards; and
3. Technical Safeguards.

There are also two additional administrative standards in the HIPAA security rule:

1. Organizational Requirements; and
2. Policies and Procedures and Documentation Requirements.

As you can see from the numerous sections of the HIPAA security regulations outlined in this introduction, only one section is specific to technology, and thus the province of your IT department. As you will learn, the HIPAA security and privacy regulations are intertwined. Many of the security decisions are business operations decisions that will need business and operational staff involvement in addition to technical staff assistance and involvement.

Implementation Specifications

Most of the HIPAA security standards come with instructions to the covered entity in the form of implementation specifications. Some of the implementation specifications are "required" and some of the implementation specifications are "addressable." Remember required implementation specifications must be implemented. Addressable implementation specifications require a covered entity to undertake a structured decision-making process. ***Addressable does not mean optional!***

Addressable Implementation Specifications

Addressable implementation specifications are one of the most confusing aspects of the final HIPAA security rule. A covered entity must determine if the addressable implementation specification is reasonable and appropriate in light of the four flexibility requirements outlined above. These are:

1. Size, complexity, and capabilities of an organization;
2. The costs of security measures;
3. The organization's current technical infrastructure, hardware and software; and
4. The likelihood that the risks will occur and the seriousness of the impact on the organization's ePHI and business operations.

The balancing of these factors is one that needs to be taken seriously and documented carefully as the addressable implementation specifications are reviewed by your practice. The choices your practice makes at this point of compliance may impact federal enforcement in the future, and possibly future litigation.

45 CFR 164.306(d)(3)(i) states that when a security standard includes addressable implementation specifications, a covered entity must:

> "Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, and … implement the implementation specification if reasonable and appropriate, or if implementing the implementation specification is not reasonable and appropriate, document why it would not be reasonable and appropriate to implement the implementation specification, and implement an equivalent alternative measure if reasonable and appropriate."

There are very few areas where a practice will not need to implement something under an addressable implementation specification. One example is a small provider that does not have any internet connections, not even e-mail. Under this circumstance, one may find some relief in the HIPAA security technical safeguards transmission standard.

Your organization may outline addressable implementation specifications decisions by:

- Differentiating required from addressable specifications;
- Assessing reasonableness and appropriateness of each addressable specification for your organization;
- Implementing the addressable specifications, or an alternative or do neither; and
- Documenting your decisions.

HIPAA Security Matrix

There is an appendix in the HIPAA Security Final Rule known as Appendix A to Subpart C of Part 164 — Security Standards: Matrix. This does not include the Organizational Requirements, the General Rules, or the Policies and Procedures and Documentation Requirements. The matrix is replicated below:

(a) Administrative Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	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	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

(b) Physical Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

(c) Technical Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312 (e)	Integrity Controls	(A)
		Encryption	(A)

HIPAA Security Maintenance

There is one more part of the HIPAA security general rules. In 45 CFR 164.306(e), HIPAA security maintenance is outlined and states "security measures implemented to comply with standards and implementation specifications adopted … (by the covered entity) must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of ePHI."

As needed means a periodic review coupled with reviews when the covered entity receives notice of a problem or a new technology that will support the HIPAA security standard.

Steps to HIPAA Security Compliance

There are three crucial steps that need to be taken to work toward HIPAA Compliance with the HIPAA Security Rule:

1. **Perform a Risk Analysis**
   - A risk analysis forms the basis for your organization's ongoing risk management. You will identify your organization's deficiencies and establish a framework to develop appropriate security measures.
2. **Select a Security Officer**
   - This seems like a simple mandate, but the person designated must participate in the risk analysis and be involved in all the ongoing security management.
3. **Develop or Update Policies and Procedures**
   - As part of your organization's risk analysis, include another column for evaluating your current policies and procedures. The gaps discovered with this review will fit into your plan to complete your HIPAA security work.

III. HIPAA Security Compliance Checklists

A. Who Is Required to Comply with HIPAA?

The HIPAA regulations apply to the following entities: health care providers who transmit any health information electronically, health plans (including Medicare and Medicaid programs), and health care clearinghouses. These groups are collectively referred to as "Covered Entities." HIPAA defines a health care provider as a provider of medical or health services or any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

You are *not* a Covered Entity under HIPAA if you do not perform *any* electronic transactions in your practice (e.g., billing, eligibility checks, referral authorization, financial transactions). If you are not a Covered Entity, then you need not comply with the HIPAA Electronic Transaction and Code Set standards and the Privacy Standards,[1] and you need not comply with the Security Standards.

Note: Under HIPAA, if you have a billing company (or any other entity) conducting electronic functions on your behalf, you are still considered to be performing electronic transactions since the billing company (or other entity) is considered an "extension" of you.

If you are *not* a Covered Entity, you may ultimately become one if you will be required to submit electronic claims to Medicare. Under the federal law, ASCA[2] providers were required to cease submitting paper claims to Medicare and to submit claims electronically by Oct 16, 2003.

Exception under ASCA: If you are a Medicare provider and have less than 10 full-time employees, administrative and clinical staff included, you meet an exception to the ASCA requirement to submit electronic bills to Medicare. You can continue to submit paper claims to your Medicare carrier after October 16, 2003.

If you are a covered entity or do not qualify for the ASCA Medicare electronic submission exception, please continue.

[1] The Office for Civil Rights HIPAA Privacy Technical Assistance 164.000.001 General Overview as visited on September 17, 2002. Last revised: July 6, 2001

[2] ASCA is a separate federal law that was signed into legislation on December 27, 2001, by President Bush. This law provides for a one-year extension for complying with the HIPAA standard transactions and code set requirements (to October 16, 2003), and requires that by Oct 16, 2003, providers billing Medicare cease submitting paper claims and instead submit claims electronically to Medicare. There are waivers for certain small providers or if there is no method for electronic submission of claims available.

B. Checklists

Before you begin, consider the size and sophistication of your office practice. The federal government has given some indication that it acknowledges that physician practices vary in size, nature of services provided, and overall administration. The HIPAA regulations and accompanying commentary include the concepts “scalable” and “reasonable.”

As you go through the following lists, questions may arise that are not answered in this booklet. This checklist should be considered a guide only, and is in no way intended to be comprehensive or a “one size fits all” evaluation for all physician practices. It is also strongly suggested that you contact your legal counsel or an attorney with expertise in HIPAA, who can review your compliance plan, including your new policies, notices, and agreements.

Further, Massachusetts has several laws that may uniquely interact with the HIPAA regulations or be preempted by them. This booklet does not cover any state-specific requirements. Compliance efforts that are well documented with legal review may be your best defense against any potential investigation.

HIPAA Security Self Assessment

Check Yes or No:	YES	NO
A Security Officer or Security Team has been appointed for your organization.	☐	☐
A job description has been developed for the Security Officer/Team.	☐	☐
The Security Officer/Team has been trained to perform the duties as identified in the job description.	☐	☐
The Security Officer/Team has been trained on the Security Policies and Procedures.	☐	☐

Response and Reporting Procedures

	YES	NO
The Security Officer/Team has established a process for reporting and identifying security questions and violations.	☐	☐
Your organization has established criteria for what constitutes a security incident.	☐	☐
Security incidents are analyzed and remedial actions are taken and documented.	☐	☐

Policies and Procedures

	YES	NO
Security Policies and Procedures have been developed.	☐	☐
The Security Management Process has been documented. (see pg 29)	☐	☐
Security Policies and Procedures are made available to applicable users and employees.	☐	☐
Security Policies and Procedures undergo annual or other periodic review.	☐	☐
Technical Security Configuration Documents exist for all major applications, such as operating systems, routers and other areas.	☐	☐
Security Requirements are included in all solicitation documents, including RFPs.	☐	☐
The decisions and reasons for not implementing addressable specifications or implementing alternatives are documented.	☐	☐
Periodic technical and non-technical evaluations are scheduled to determine compliance with policies and procedures.	☐	☐

Computer and Network Management

	YES	NO
Network Security Mechanisms, such as firewalls, have been implemented.	☐	☐
Virus Detection Systems have been installed.	☐	☐
Virus Signature Files are routinely updated.	☐	☐
Intrusion Detection Systems are installed on appropriate systems.	☐	☐
Prevention Testing is performed on the system.	☐	☐
Integrity Controls have been implemented to prevent improper alteration or destruction of PHI.	☐	☐
An Information System Activity Review is regularly performed.	☐	☐
An Inventory System for all hardware and software is implemented.	☐	☐
Movement of all electronic devices, including hardware, is tracked within the organization.	☐	☐
Data Backup or Storage is conducted before moving equipment.	☐	☐
Inventory Logs are periodically reviewed and updated.	☐	☐
Workstation Procedures are established for each type of workstation, including procedures for both equipment and the physical surroundings or the workstation.	☐	☐
Transmission Security Measures are in place to protect ePHI transmitted over communication networks.	☐	☐
Audit Controls are in place to record and examine information systems containing ePHI.	☐	☐

Updates and Maintenance

	YES	NO
Security Requirements are identified for all new system designs.	☐	☐
Risk Assessments on all new or updated systems are performed.	☐	☐
System Documentation is modified as changes to systems occur.	☐	☐
System Maintenance Plans are developed and implemented on a regular basis.	☐	☐
Maintenance records to document repairs and modifications to the physical components of a facility related to security are maintained and updated and reviewed on a continual basis.	☐	☐

Authorization for software modifications is obtained and documented.	☐	☐
New and Revised hardware and software are authorized and tested before implementation.	☐	☐
Distribution of new software is documented.	☐	☐
Data backup and storage are performed before maintenance or updates.	☐	☐
Risk Determinations are documented.	☐	☐
Impact Analyses have been conducted and documented.	☐	☐

Disposal

	YES	NO
Disposal Procedures for ePHI are established.	☐	☐
Disposal Procedures are established for specific types of media, such as hardware, CD, and all others.	☐	☐
Disposal Records are maintained and verification of proper disposal is documented.	☐	☐
Paper media is destroyed when it is no longer needed.	☐	☐
Procedures for the re-use of media and devices that previously contained ePHI have been established.	☐	☐

Contingency Planning

	YES	NO
A Contingency Plan for your organization has been developed, tested, and implemented.	☐	☐
The Contingency Plan is reviewed periodically and updated as needed.	☐	☐
A Disaster Recovery Plan has been developed, tested, and is in place.	☐	☐
Responsible parties have been provided detailed procedures and training for their assigned duties under the Contingency and Disaster Recovery Plans.	☐	☐
A copy of both the Contingency Plan and the Disaster Recovery Plan are in a secure location.	☐	☐
Data Criticality Analyses are performed where necessary to assess the relative criticality of applications and data.	☐	☐
Does your organization have a data back up plan? (see also pgs 16–18)	☐	☐

Does your organization have an emergency mode of operations plan? (see also pg 20)	☐	☐
Does your organization have a facility security plan? (see also pg 21)	☐	☐

Training and Education

	YES	NO
Employees have been trained on all applicable Security Requirements for their job functions.	☐	☐
Security Requirements are communicated to staff on a regular basis.	☐	☐

Risk Management

	YES	NO
An Initial Risk Analysis is conducted to assess potential risks and vulnerabilities.	☐	☐
Risk Assessments are performed and documented on a regular basis or when changes occur.	☐	☐
Threat sources have been identified and classified.	☐	☐
Risk determinations are documented.	☐	☐
Impact Analyses have been conducted and documented.	☐	☐

Access Controls

	YES	NO
Access Controls are used for all sensitive systems, files, and directories.	☐	☐
Password Management procedures are used.	☐	☐
Unique User Identification for identifying and tracking individuals is assigned to each user.	☐	☐
Remote Connections into the organization's network are secured.	☐	☐
User Privileges are based on job functions or employee classification.	☐	☐
Access is granted based on valid business needs.	☐	☐
User Privileges are revoked when an employee is terminated.	☐	☐
User Privileges are modified when an employee's job description or classification changes.	☐	☐
Emergency Access Procedures have been established for accessing	☐	☐

ePHI information during an emergency.

Automatic Logoff Procedures have been implemented.	☐	☐
Authentication procedures are implemented to ensure the person or entity seeking access is the one claimed.	☐	☐
If encryption is used, proper procedures are followed for database, password, and file encryption.	☐	☐

Physical Security

	YES	NO
Facility Access Control Procedures have been implemented to limit physical access to ePHI and facilities where it is housed.	☐	☐
Facility Security Plans have been developed and documented.	☐	☐
Periodic reviews of Facility Security Plan(s) have been scheduled.	☐	☐
Access to facilities is controlled through identification or key cards.	☐	☐
Contingency plans allow access to the facility for purposes of restoring lost data.		
Visitor identification is required throughout the facilities.	☐	☐
Keys, keycards, and other access devices are assigned and logged.	☐	☐
Keys or other access devices are required for sensitive areas such as server rooms.	☐	☐
Unused keys and access devices are properly secured.	☐	☐
Computers, fax machines, and printers are placed in areas that are not easily accessible to unauthorized persons.	☐	☐
Portable systems such as laptops are properly secured.	☐	☐

Workforce Security

	YES	NO
Authorization procedures are followed for workforce members requiring access to ePHI.	☐	☐
Clearance procedures are followed when determining access of employees.	☐	☐
A Sanction Policy has been developed to apply appropriate sanctions to workforce members who do not comply with security policies and procedures.	☐	☐

Business Associates

	YES	NO
Business Associate contracts are in place with all business associates who create, receive, maintain or transmit ePHI (this is beyond the HIPAA privacy business associate contract).	☐	☐
Satisfactory assurances are obtained from business associates that they will appropriately safeguard information.	☐	☐
A definition as to what constitutes satisfactory assurance has been developed and documented.	☐	☐
In cases where Business Associate contracts are not applicable, other arrangements are made between organizations and the business associate to keep data confidential.	☐	☐

Practical Security Policies and Procedures

	YES	NO
Does your organization have e-mail and ePHI policies and procedures?	☐	☐
Does your organization have fax and ePHI policies and procedures?	☐	☐
Does your organization have laptop and ePHI policies and procedures?	☐	☐
Does your organization have PDA and ePHI policies and procedures?	☐	☐
Does your organization have Instant Messaging policies and procedures?	☐	☐

IV. Pointers for Drafting Your HIPAA Security Risk Analysis

First Steps — Build a Team

As a practice begins to prepare for HIPAA security compliance, one of the first steps is to meet with your organization's HIPAA privacy compliance team. You should discuss the privacy team's findings and frustrations. This way you will not duplicate efforts and you will learn from the plusses and minuses of the privacy implementation. Also, you may find that your privacy team already has a list of items that may not be security issues directly, but relate to the security standards.

Your second step should be to identify your team. One of the first administrative standards is to appoint a security official who is assigned security responsibility. 45 CFR 164.308(a)(2).

The standard states "identify the security official who is responsible for the development and implementation of the policies and procedures … for the entity." This section directs that one individual must be the owner and facilitator of the security policies and procedures, and it is suggested that the policy manual include other documentation.

This team requires many of the same roles as your team for privacy compliance.

Consider enlisting the participation of the following individuals, or individuals that have the following skill sets:

1. The Security Official;
2. At least one strong writer;
3. Someone responsible for training and communication;
4. Several systems representatives aside from the Security Official;
5. The Privacy Official;
6. Operations representatives;
7. Regulatory and legal representation;
8. Facilities/building maintenance and management;
9. Human resources;
10. Medical or clinical staff representative;
11. If in a hospital, a member of the safety committee; and
12. Others who will have ongoing ownership for each policy and procedure.

Once you get your team together and have an initial meeting with your organization's privacy compliance team, you need to take a couple of initial steps to set your foundation.

If you are a larger physician group, consider the development of a security charter that would include a vision statement, a mission statement, and a values statement.

Set sponsorship within your organization and a responsibility of chair.

Sponsorship and Responsibility

It must be understood that management's responsibility under the HIPAA security rule goes well beyond securing the physical environment and the technology infrastructure. Security policies and procedures must be established, implemented, maintained, and enforced throughout the workforce. The Security Compliance/Implementation team must manage the organizational change in the culture and beliefs in this area as much or even more than for the HIPAA privacy rule requirements.

Management has the lead role in the following tasks:

1. Define the vision of the security framework — including all aspects of the technology infrastructure;
2. Define the level of security the practice requires in relation to the security rule requirements — this is the specific practice's balance and criteria for risk establishment;
3. Develop the plan that will create the administrative processes and security procedures for the practice — this is the road map for making the decisions and implementing the decisions;
4. Provide the budget needed to implement the security level specifically defined by the practice;
5. Require all workforce to comply with the HIPAA security regulations;
6. Empower the lower-level management to enforce security policies and procedures; and
7. Develop a reporting and enforcement process and structure to ensure security policies and procedures are followed.

HIPAA Security and Budgeting

Historically health care organizations have not spent much money on information technology (IT). Other industries have computed an expected return on investment (ROI) coupled with a risk analysis for not taking certain actions. Health care is just beginning to grasp these concepts. The first HIPAA Security administrative safeguard is the security management process that includes risk analysis, risk management, a sanction policy, and information system activity review.

A risk analysis is required. A practice must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

Risk management is also required. A practice must "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level …"

Most health care organizations have not been successfully hacked, despite what one reads in the press or what is posted on the privacy websites. However, these types of incidents are increasing. The HIPAA security team must make a good case for effective and appropriate security within the organization.

The budget for HIPAA security must incorporate the cost of all the equipment and labor to draft and/or implement as well as maintain the enterprise-wide security solutions to protect ePHI.

For software this includes:

- Initial software costs;
- Future annual maintenance costs; and
- Additional costs of equipment to support the solutions.

The labor includes:

- Drafting, implementing, and maintaining policies, procedure, and plans; and
- Installing, updating, and maintaining software and hardware.

In other words, the following must be included in planning:

- All workforce must be involved in this effort;
- Coverage of the tasks and jobs to be back-filled during this period; and
- Consultant labor to implement, train, or maintain your security solutions, if applicable.

This process should be accompanied by an ROI Analysis and Benefits Analysis for security solutions implementation and maintenance.

Essential and Best Practices

The development and implementation of detailed and specific security policies provides the basis for good security practices. The security policies developed by a practice will vary due to the balancing of numerous factors outlined in the introduction above, including, but not limited to, differences in purpose, size, budget, and information systems architecture.

There are a number of areas and issues to consider when developing your practice's security policies and procedures, including:

- Identifying IT systems, software programs, and other media that store or use ePHI;
- Identifying the vendors who provide the identified systems and asking them specific HIPAA security questions;
- Gathering all current security policies and procedures, and any related privacy policies and procedures;
- Gathering all security plans, such as contingency or emergency mode operations plans;

- Developing lists of actions that are a violation of your security system and disciplinary actions and sanctions when the security system is violated;
- Determining where the policies and procedures will be maintained and who will be the owner of the policies and procedures;
- Determining a process for approval of policies and procedures, as well as revision; and
- Checking the policies and procedures against each other, including your privacy policies and procedures, for consistency and validation.

A practice must assess its technology, including:

- Web servers;
- Applications systems;
- E-mail;
- Network infrastructure;
- Operating systems;
- Databases;
- Intrusion detection;
- Firewalls; and
- Anti-virus software.

A practice must assess its physical environment and people, including:

- Bulletin boards;
- Cleaning personnel and other similar work staff;
- Visitors;
- Computer screens;
- Copy machines;
- Printers;
- Fax machines;
- Desks and countertops;
- Disposal of paper;
- Home office;
- Information carried from one facility to another;
- Keys and other locks;
- PDAs and laptops;
- Records storage; and
- Transcription.

A practice must consider all of its assets/resources, including:

- Telecom;
- IP/Web servers;
- Electricity;
- Heat and air conditioning;
- Oil;
- Generators;
- Supplies of all kinds;

- Couriers; and
- US Mail.

A practice must consider its special conditions including:

- Weather;
- Type of services provided; and
- Type of governance (business structure or model).

HIPAA Security Management

Both the HIPAA privacy and security rules require a practice to take any "appropriate and reasonable" measures to "ensure" and "safeguard" the individual's PHI. There are administrative, physical, and technical safeguards in both rules.

The administrative safeguards within the security rule are administrative actions, policies, and procedures and plans related to the selection, development, implementation, and maintenance of security measures. They also address managing the conduct of your workforce.

In some health care organizations, health care information management is fragmented and inconsistent. Yet inherent in the security rule is the requirement that covered entities recognize and operate in a cohesive, synergistic manner. This is a change from the current makeup of many operations, where departments often function as separate organizations. Thus, the HIPAA security rule anticipates and requires a cultural change to "ensure" the confidentiality of the ePHI.

Security Management

The first administrative security standard requires a practice to create, administer, and oversee a security management process (i.e., policies and procedures) to prevent, detect, contain, and correct security violations. 45 CFR 164.308(a)(1). This security administrative standard is the backbone and the foundation of all HIPAA security and the final HIPAA security rule.

The security management process has four implementation specifications as follows:

1. Risk analysis and assignment;
2. Risk management;
3. A sanction policy; and
4. Information system activity review.

Risk Analysis

A risk analysis is the first implementation specification of the HIPAA security management process standard. It is found at 45 CFR 164.308(a)(1)(ii)(A).

A risk analysis was defined in the HIPAA security proposed rule, but was omitted from the final rule. It was defined as:

> Risk analysis is a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.[3]

There is no explicit definition in the final HIPAA security rule. The preamble to the final rule does state that covered entities must look at all "relevant losses."[4] Relevant losses can include unauthorized uses and disclosures and loss of data integrity that would occur without appropriate security measures.

Your risk analysis must:

1. Identify your tools that hold ePHI;
2. Identify the threats to that ePHI;
3. Identify the vulnerabilities in your system that would permit these threats to impact your ePHI;
4. Identify what the loss or destruction of ePHI would mean to your organization; and
5. Identify what controls your organization can put in place to protect your ePHI.

A hardware and software risk assessment should include:

1. All servers;
2. Your entire network, including:
   - Topology;
   - Local area networks;
   - Wide-area networks;
   - Communication servers;
   - Bandwidth connectivity; and
   - Storage;
3. All databases with ePHI; and
4. All computers connected to ePHI for data processing and analysis.

[3] HIPAA Security NPRM, page 43275
[4] HIPAA Security Final Rule, page 8347

A systems inventory should include:

1. All policies and procedures that impact the security of ePHI;
2. All information systems with a focus on critical/sensitive ePHI processed by these systems;
3. All business associates and how they process/use ePHI;
4. All biomedical equipment that contains ePHI;
5. All employees that have remote access *of any kind* to ePHI; and
6. All vendor partners who have access to ePHI.

After all your data has been collected and analyzed, perform a gap analysis to identify your areas of exposure and/or vulnerabilities within each area and how they interconnect. This will assist you in predicting the probability of occurrence and the loss with a catastrophic security breach.

In the end, your risk analysis should demonstrate, at a minimum, the following:

- The risk level associated with each potential vulnerability;
- Steps to be taken to reduce such vulnerability; and
- The processes to maintain no more than the acceptable level of risk.

Assigning Risk

A risk assignment should include:

- Analysis of loss potential;
- Analysis of your user community;
- Workforce security;
- Analysis of the attack including probability, type, and source of attack;
- Level of security;
- Ease of use and access;
- Cost/benefit analysis for each solution; and
- Coordination of each solution to your contingency plan.

What level of security incidents is acceptable? This is the question a covered entity must ask itself when it is determining its comfort zone. In other words, you must quantify your potential losses. After your risk analysis you will be aware of the holes in your security infrastructure, your most vulnerable areas, and the probable impact if the ePHI was lost or compromised.

Not all ePHI is of equal value or sensitivity. After providing a baseline security for all ePHI, you can create a hierarchical prioritization of the more valuable and sensitive ePHI by department in your organization.

A covered entity's user community will outline the complexities of the flow of the ePHI on a daily basis.

For instance, does your workforce have access to the internet?

The internet is an increasingly used environment for clinicians as a standard tool. Laptops, PDAs and other, similar tools are now in the hands of many clinicians. Often these systems have no security and no encryption, and quite often no virus protection. Many clinicians do not understand the security risks associated with using such a tool to transmit ePHI, and often introduce these tools into your environment without your notice. Many managers allow unrestricted usage across the internet and open portals. This is a peril in the HIPAA Security environment.

Do you permit input of original ePHI by a clinician from a remote site?

Clinicians access, make changes to, and update ePHI from their home PCs. This is an unsecured environment. The access may be through an open internet portal. The PC may be a family tool that a spouse and/or children have access to. The clinician may write ePHI onto a disk or burn in onto a CD using his or her home PC. He or she may also download programs from their home PC or from an internet site and upload them onto his or her worksite PC at the office or your hospital. This is one way viruses walk into a health care organization network.

Do you use the internet as a communication link?

Many health care organizations use the internet as a communication link instead of installing a VPN or a WAN, especially if the organization is far flung and made up of many pieces (for example, a hospital, several practices, a nursing home, and ambulatory services that combine into one health care organization). Is your practice part of a WAN?

Do you upload ePHI from external locations?

Many health care organizations upload ePHI from a number of unsecured external locations such as home PCs, an outside vendor, or from locations not designated to handle this sensitive information.

Do you have downtime procedures for the export and importation of PHI?

Do you revert to paper when your system is down? Often there are no security provisions for this type of operation. Security should be the same for the uploading and downloading of ePHI when done from electronic tools and when paper files are used.

Do you exchange ePHI with associated health care organizations?

Many health care organizations exchange PHI with other treating health care entities for the same patient. This is the opposite of downtime. These tasks, until recently, had been handled mostly by fax and courier where there were appropriate controls. Now that the exchange of PHI is being done electronically, similar security controls are often not considered at implementation. Often the initiating health care organization is unaware of who is receiving, reviewing, and using the PHI.

Workforce security is often not one of the areas practices consider when they are considering new security measures. Your workforce is both your greatest strength and your greatest weakness. A number of studies in the late 1990s showed that the main issues and problems in security are people, next people, third people, and last people; in other words, internal staff, former staff, visitors, and hackers. As a result, a practice will need to establish personnel clearance procedures that may include background checks for the staff members who handle the most sensitive PHI. You will also need to update areas of access and issue security codes.

The new security procedures must be uniformly enforced. These procedures should become part of a continuous updating process, part of your maintenance, and part of your ongoing training. An organization cannot absolutely guarantee that there will be no security incident, but a practice can — and must — put their best efforts forward in preventing a security incident by ensuring their entire workforce of management, system users, clinicians, and IT maintenance staff receive ongoing security awareness training as technologies and organization IT changes occur.

A very important part of security risk analysis is to understand the potential attacks, the probability of attack, the type of attack, and the source of the attack. The issue is not if you will be attacked, but when, how often, and by whom. Your probability will increase each time ePHI leaves your network and is open to the public through the internet.

The most common type of external attacks are from worms, viruses, and when you leave a gateway from your network open to the internet. External attacks arrive on disks brought into your organization by workforce. Internal attacks are mostly intrusion attacks from health care workers who are attempting to obtain information on patients under care. Another internal attack is the destruction of information by angry members of your workforce who have access to the system.

The level of security within a practice is a balancing between the requirements and the resources of people, money, time, and space. A major limit that impacts these decisions is the budget for security. User access is also an important part of the decision. Usually the more sophisticated security measures are not known as user-friendly. Another problem is the possibility of incompatibility of the new security measures with your existing technology and infrastructure. Finally, if your management is unwilling to invest in security solutions and to implement and enforce policies and procedures, your level of security may not be sufficient to comply with HIPAA security requirements.

One important issue that needs to be considered with new security measures is ease of use and ease of access to the ePHI. You must consider your main mission of providing medical services to as many patients a day as you can process. An efficient system will permit a doctor and other clinicians to see more patients per day, but is it secure?

If the system is too secure and is not user-friendly, the workforce will devise a paper or technical work-around that may skirt all the security measures. You do not want this to happen. Remember, you can build a vault and the workforce will not keep any ePHI in it or you can build

an infrastructure that has keys that will permit the workforce with the appropriate capabilities to open the door and obtain the ePHI necessary to their jobs and tasks.

You cannot expect a clinician to wait two minutes for access to the ePHI. This would ripple up to three hours a day if he or she enters the system 90 times a day. This is a reasonable expectation in many busy doctors' offices and ambulatory and in-patient hospital settings.

Do you need a cost/benefit analysis for each security solution? This is a very good idea — especially in a tightly budgeted health care organization. Such an analysis should include all costs to acquire, implement, and support the security solution. For benefits, it would need to include the hard-dollar benefits such as savings in downtime and associated loss of revenue, and soft-dollar benefits such as loss of productivity.

Your security solutions should be cross-mapped to your contingency plan, especially the sections that address the emergency mode of operation. Your technology solutions should be cross-mapped to your business operations solutions of policies and procedures.

You should add some metrics to your risk assignment that are specific to your health care organization. The business risk can be high, medium, or low. You can assign some metrics to implementation at your current baseline level, such as nothing in place currently, a little in place currently, an acceptable level is in place for your practice, or you may have a great deal in place that is fully integrated into your systems and plans. In addition, you may note if you have documentation on this security measure including a policy, procedure, or plan. You may also note if the security measure, if not implemented, is in the budget. Last but not least, you may assign a priority for implementation.

Risk Management

The second implementation specification under the HIPAA security management process standard is risk management. It is found at 45 CFR 164.308(a)(1)(ii)(B).

Risk management is the process of assessing the risk, taking steps to reduce the risk to a reasonable and appropriate level for compliance purposes, and maintaining this acceptable level of risk. Thus, risk management is not a one-time event; it is an ongoing process as technology changes, the services your practice provides change, and HIPAA regulations change.

The risk analysis and the risk management requirements of the HIPAA security standards form the foundation for the remaining standards and implementation specifications in the rule.

To begin, a practice must use the findings of the risk analysis to create a HIPAA security infrastructure to manage the risk factors on an ongoing basis.

For your risk management you need to consider:

- The risks in each department/area including downtime, distribution of ePHI, and incorrect ePHI;
- Risk prioritization;
- Process to reduce risk;
- Infrastructure to maintain lower level of risk; and
- Escalation process.

You will need to assess the risk of each work area, department, or division. One risk your HIPAA security team will need to consider is downtime. You may prioritize the risk of each work area, department, or division according to the impact of downtime in relation to the rest of your organization, patient safety, and the user community. In a hospital or a clinical practice the downtime is also impacted by the work being done and the immediacy of need of the ePHI in the systems. For instance, downtime in electronic patient records for patient treatment would rate a higher priority than downtime in HR or accounting.

Another area of risk is the distribution of ePHI. Practices keep ePHI distribution lists on paper as well as electronically. The ePHI lists are adjusted, updated, and reset with the addition and removal of workforce from the systems within the practice.

EPHI lists can cause improper distribution of ePHI to unauthorized personnel. For example, a nurse works in three major areas of a hospital. Her major job is as a nurse manager in the ER. In this work mode she may need access to a deep amount of clinical ePHI to deal with unconscious patients. Some evenings she is called to work the pediatric floor, as this is where she began her nursing career and she enjoys this a few days a month. In this work mode she needs access to a great deal of clinical information about a small group of patients. On weekends she works doing claims review. In this mode she is performing a business task, not a clinical task, and needs access to billing and procedure information. In this case, the nurse needs a wide range of access to ePHI to complete her job(s).

The security industry suggests that improper distribution of ePHI to unauthorized personnel can be as big, or an even bigger risk, than downtime.

The entry of incorrect patient information into a patient chart, medical record, or business record is another area of risk. The opposite risk is the deletion of patient ePHI. These risks impact the health and care of patients. Imagine having a son's information in a file of the father, the son being Junior. The absence of completely accurate information often poses irredeemable risks. We have all heard the story of the surgeon who operated on the wrong side of the patient.

The next step is to prioritize your risks. You should consider the following questions as you prioritize your practice's risks:

- Impact of downtime to work area, department, or division?
- Impact of distribution of ePHI to inappropriate personnel?
- Impact of incorrect ePHI or deletion of ePHI?
- Potential patient endangerment?

- Impact to general flow and integrity of ePHI?
- Impact to other parts of your health care organization?

Once your practice has prioritized the risks, you will need to create a process to remediate and reduce the risks. You must outline where there are current gaps in your security and use process, policy and procedure, technology, and training to fill the gaps. You need to outline the ramifications and interdependencies for other work areas, departments, and divisions within your health care organization.

One question you need to ask is: are the risks and/or gaps only in one or certain work areas, departments, or divisions? You may categorize risk by department, work task, or job as well as physical area or technology gap. Risks almost always have complexities as you work to correct the security gap and processes. Who is connected to and dependent on this ePHI? What is the budget to correct the risk, both in money and in people? What is the total cost to cure the risk?

Your practice may fill the gaps and cure the risks by:

- Updating technology;
- Drafting new policies and procedures;
- Updating or creating new processes;
- Workforce training; or
- A combination of above.

Once your practice has filled its initial gaps and cured its immediate risks, you will need to have an infrastructure in place to maintain this lower level of risk that you have taken the time to draft, create, and implement. You may create a small dedicated team or committee with members from IT, executive management, and your end users as this infrastructure. Remember, it should reach all parts of your organization, and with end users on your security team, you will gain buy-in throughout your organization.

This team will set the rules that will create ongoing security and give easy access to the user community as they will be involved in the decisions and the evolution of your security structure.

The team should keep in mind that the rules they create must be easy to implement throughout the organization. It is key to remember that all the work areas, departments, and divisions must be able to live with these rules. These rules will be no good if they do not work across the organization. These are your baseline security rules, not the special rules for your special areas such as research.

Additionally, this team will create the final draft of the rules that will become the universal policy within your health care organization. As you work on this draft set of policies and procedures, get sign-off by all work areas, departments, and divisions. This way, all affected parties will be involved and on notice from the beginning of the project.

Sanction Policy

One important area of the HIPAA security rules is sanctions. The team will also develop and lay out a progressive escalation of penalties, and create an enforcement escalation process that includes executive management sign-off for the most egregious behavior and willful actions. Finally, it is suggested that all workforce sign off on the new sanction policy, the penalties, and the escalation process so they know that HIPAA makes everyone who works with patient PHI responsible for keeping it secure and private.

The escalation process outlined above must be implemented in each work area, department, and division of your health care organization. You may have a process to alert, report, and escalate a security breach to the work area supervision, or the department or division leader. It is suggested that you train yearly in this process of reporting a security violation. The training should outline whom to first call and the hierarchy of contact and notification as the security risk is escalated. The training should also outline the timing between each phase of escalation and what triggers the next level of notification. Examples and illustrations of inappropriate behavior and misdeeds need to be part of the training.

You need to determine the following as you develop this escalation process:

- When is it appropriate to make the first call — the level of intrusion or improper release of PHI;
- Whom first to call — name the role and not the individual — and when to call (the timeframe);
- What is the escalation trigger, what is the escalation time; and
- Are there any escalation events for the next level, or just time elapsed?

Information System Activity Review

The fourth implementation specification for the security management is information system activity review. It can be found at 45 CFR 164.308(a)(1)(ii)(D).

It mandates that a practice "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

This mandate assigns responsibility to a practice so they know what is going on in their systems that maintain and transmit ePHI. It is a requirement to ensure the security of your ePHI.

The administrative mandate is looking for procedures such as review schedules and reporting, plus escalation up the hierarchy for progressively deeper risks.

The technology of system audit logs, access, and reports, plus security incident tracking are part of the HIPAA security technical safeguards.

V. Pointers for Drafting Your HIPAA Security Policies and Procedures

Documentation — Policies, Procedures, Plans

The HIPAA security rule has a policy and procedure documentation mandate that parallels the one found in the HIPAA privacy rule. It is found at 45 CFR 164.316. The standard states that a practice must implement "reasonable policies and procedures to comply with the standards, implementation specifications, and other requirements" of the security rule.

The security rule policies, procedures, and plans include:

- Policies and procedures to prevent, detect, contain, and correct security violations
- Sanction policy
- Procedures to regularly review records of information system activity
- Policies and procedures to ensure that all members of a covered entity's workforce have appropriate access to ePHI
  - Procedures for authorization and/or supervision of workforce members who work with ePHI or in the location where it may be assessed;
  - Procedures to determine that access of workforce to ePHI is appropriate; and
  - Procedures for terminating access to ePHI when employment ends.
- Policies and procedures for authorizing access to ePHI:
  - Policies and procedures to isolate a health care clearinghouse functions from unauthorized access by the larger organization;
  - Policies and procedures for granting access to ePHI; and
  - Policies and procedures to establish, document, review, and modify a user's right of access.
- Policies and procedures for responding to an emergency or other occurrence that damages ePHI contingency plans:
  - Data back-up plan — Procedures to create and maintain retrievable exact copies of ePHI;
  - Disaster recovery plan — Procedures to restore any loss of data;
  - Emergency mode operation plan — Procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode;
  - Procedures for periodic testing and revision of contingency plans.
- Policies and procedures to identify and respond to suspected or known security incidents:
  - Procedures to mitigate, to the extent practicable, known harmful effects from the incident;
  - Documentation of security incidents and their outcomes.

The requirements within 45 CFR 164.316 include:

- Maintaining the policies and procedures in written or electronic form;

- Retaining the documentation for six years from the date of its creation or from the date of revision or date when last was in effect, whichever is later[5];
- Making documentation available to persons responsible for implementing the procedures and plans; and
- Reviewing documentation periodically and updating as needed (e.g., in response to environmental or operational changes affecting the security of ePHI).

The following is a Policy Manual Checklist. Please remember that this checklist is to be used as an educational tool only to assist you as you begin drafting your own HIPAA office policy manual. It is in no way intended to be a comprehensive guide in complying with the HIPAA Security Regulations.

HIPAA Security Policies and Procedures Checklist

	YES	NO
Does your organization have risk assessment and ongoing risk management policies and procedures?	☐	☐
Does your organization have security sanctions policies and procedures?	☐	☐
Does your organization have activity review or information system security policies and procedures?	☐	☐
Does your organization have assignment of security responsibility policies and procedures?	☐	☐
Does your organization have workforce clearance policies and procedures, including authorization and/or supervision?	☐	☐
Does your organization have termination and modification of access to PHI policies and procedures, including facility controls and electronic systems?	☐	☐
Does your organization have a security awareness and training for safeguarding ePHI, including policies and procedures?	☐	☐
Does your organization have security incident procedures, including procedures for response and reporting?	☐	☐
Does your organization have policies and procedures for contingency planning response to unexpected negative events?	☐	☐
Does your organization have policies and procedures for evaluation of your security of ePHI?	☐	☐

[5] This is one area where you need to check your state law; in many states the time for document retention is different from the federal requirement.

	YES	NO
Does your organization have a policy for the continual update and review of your security policies and procedures?	☐	☐
Does your organization have policies and procedures for assignment of facility access controls and privileges?	☐	☐
Does your organization have policies and procedures and guidelines for workstation use and security?	☐	☐
Does your organization have policies and procedures for device and media controls?	☐	☐
Does your organization have access control policies and procedures?	☐	☐
Does your organization have audit controls policies and procedures that record and examine information systems activity that contain ePHI?	☐	☐
Does your organization have policies and procedures if ePHI has been improperly altered or destroyed?	☐	☐
Does your organization have authentication of person or entity policies and procedures?	☐	☐
Does your organization have electronic transmission of ePHI policies and procedures?	☐	☐
Does your organization have a review process for business associate agreements that includes HIPAA security?	☐	☐

Education & Awareness Training

Like the HIPAA privacy rule, there is a requirement in the HIPAA security rule for a practice to provide its workforce with security awareness and training.

It is found at 45 CFR 164.308(a)(5), and states a practice must "implement a security awareness and training program for all members of its workforce (including management)."

The requirements include:

1. Periodic security updates;
2. Procedures for guarding against, detecting, and reporting malicious software;
3. Procedures for monitoring log-in attempts and reporting discrepancies; and
4. Procedures for creating, changing, and safeguarding passwords.

Appendix A: Website Links

Websites	Information Available
Government Sites	
Centers for Medicare and Medicaid Services (CMS) www.cms.hhs.gov/hipaa/	Final HIPAA Security, Electronic Transactions and Code Sets, and Unique Identifier Regulations and Standards, Educational Papers, FAQs, Enforcement information
U.S. Department of Health and Human Services http://aspe.hhs.gov/admnsimp/index.htm	Final and Proposed HIPAA regulations, and HIPAA updates
Office For Civil Rights http://www.hhs.gov/ocr/hipaa/	Guidance documents, Technical Assistance, Privacy Updates, Complaint Process information
Electronic Transaction and Code Sets	
WEDI/SNIP http://snip.wedi.org/	Workgroup efforts to collaborate implementation strategies, Regional Workgroup updates, Issue Tracking
Washington Publishing Company http://www.hipaa.wpc-edi.com	Transaction Standards, Implementation Guides
General Resources	
Massachusetts Medical Society http://www.massmed.org	Articles relating to HIPAA compliance, weekly HIPAA Tips, MMS testimony on federal regulations
American Medical Association http://www.ama-assn.org	HIPAA updates, Model Forms
Massachusetts Health Data Consortium http://mahealthdata.org	HIPAA events, HIPAA resource library

Appendix B: Definitions

Access — in the context of the final Security rule, means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative safeguards — administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronically protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Authentication — the corroboration that a person is the one claimed to have access.

Availability — data or information is accessible and useable upon demand by an authorized person.

Business associate —

1. Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who:
   a. On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs or assists in the performance of:
      i. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
      ii. Any other function or activity regulated by this subchapter; or
   b. Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
2. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(b) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(b) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
3. A covered entity may be a business associate of another covered entity.

Code set — any set of codes used to encode data elements such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A *code set* includes the codes and the descriptors of the codes.

Compliance date — the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Confidentiality — data or information is not made available or disclosed to unauthorized persons or processes.

Covered entity —

1. A health plan.
2. A health care clearinghouse.
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure — the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic media — the mode of electronic transmission. It includes the internet (wide-open), extranet (using internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions physically moved from one location to another using magnetic tape, disk, or compact disk media.

Encryption — the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility — the physical premises and the interior and exterior of a building(s).

Health care — care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse — a public or private entity, including a billing service, repricing company, community health management information system, or community health information system, and “value-added” networks and switches, that perform either of the following functions:

1. Process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
2. Receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider — a provider of services (as defined in section 1861(u) of the Social Security Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Social Security Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information — any 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.

HHS — stands for the Department of Health and Human Services.

Implementation specification — specific requirements or instructions for implementing a standard.

Individual — the person who is the subject of protected health information.

Individually identifiable health information — information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, 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; and
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information system — an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity — data or information have not been altered or destroyed in an unauthorized manner.

Malicious software — software — for example, a virus — designed to damage or disrupt a system.

Password — confidential authentication information composed of a string of characters.

Physical safeguards — physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Protected health information — individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   a. Transmitted by electronic media;
   b. Maintained in any medium described in the definition of electronic media (see above); or
   c. Transmitted or maintained in any other form or medium.
2. Protected health information excludes individually identifiable health information in:
   a. Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and
   b. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
   c. Employment records held by a covered entity in its role as an employer.

Security *or* **Security measures** — encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident — the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Standard — a rule, condition, or requirement:

1. Describing the following information for products, systems, services or practices:
   a. Classification of components;
   b. Specification of materials, performance, or operations; or
   c. Delineation of procedures.
2. With respect to the privacy of individually identifiable health information.

State — refers to one of the following:

1. For a health plan established or regulated by Federal law, *state* has the meaning set forth in the applicable section of the United States Code for such health plan.
2. For all other purposes, *state* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Technical safeguards — the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Transaction — the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Other transactions that the Secretary of Health and Human Services may prescribe by regulation.

Use — with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User — a person or entity with authorized access.

Workforce — employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Workstation — means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.