HIPAA: Health Insurance Portability and Accountability Act

Publication details
Ross A. Leo
Published online on: 29 Dec 2015

How to cite: Ross A. Leo. 29 Dec 2015, HIPAA: Health Insurance Portability and Accountability Act from: Encyclopedia of Information Systems and Technology CRC Press
Accessed on: 19 Aug 2023

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
HIPAA: Health Insurance Portability and Accountability Act

Ross A. Leo
Professional Training and Development, University of Houston-Clear Lake, CyberSecurity Institute, Houston, Texas, U.S.A.

Abstract

The “Health Insurance Portability and Accountability Act,” commonly referred to as HIPAA, and its amendment known as “Health Information Technology for Economic and Clinical Health (HITECH),” have been heralded as bringing vital attention to the matters of the privacy and security to patient information. They have also brought controversy to the general discussion of information protection, its cost, the associated burden of program management, breach reporting, and related topics. Over time, much has been clarified but much remains to be clarified before truly effective and cost-efficient programs can be designed and institutionalized. This entry will address these issues and provide more clarity on how to achieve the objective for protecting the privacy and security of patient information. It will lay the foundation for defining IT controls, the objective of each, implementation and operational guidance, and the interdependence of them. It will provide examples of effective options to achieve the goals without breaking the bank or adversely impacting the delivery of timely, appropriate, and high-quality healthcare. It will enlarge on the requirements of these important laws, their impacts on the IT portions of an affected enterprise, and will elaborate on the manner in which they must be addressed so that this vital program of protection can be brought about quickly and efficiently, without excessive cost or adding unacceptable overhead, in an evolutionary, not revolutionary manner.

OVERVIEW

This entry will discuss the “Health Insurance Portability and Accountability Act,” commonly referred to as HIPAA (Public Law 104-191, 1996), including the amendment known as “HITECH,” which is a specific portion (Title XIII, Subpart D) of the American Recovery and Reinvestment Act of 2009 (ARRA), and the Omnibus Rule issued in January of 2013.

The entry will enlarge on the requirements of these important laws, their impacts on the IT portions of an affected enterprise, and will elaborate on the manner in which they must be addressed when an entity works to comply with them. All security measures, concepts, functions, and controls reflect current best practice endorsed by all certification bodies and government organizations.

Within this legislation are four primary categories of controls: Administrative, Physical, Technical, and Organizational. This entry focuses on those related to the Information Systems processing the covered data types, but will address the Physical and the Organizational as well in terms of their impact on these systems and data.

BACKGROUND OF THE LEGISLATION

This legislation was signed into law by President William J. Clinton in August of 1996. Its intended goals included:

a. Administrative simplification in the processes used in handling healthcare information by creating types and functions of “transactions,” standardizing messaging formats, exchange mechanisms, and process participants;

b. Combat fraud, waste, and abuse of the claims process which often resulted from millions to billions of dollars in payments on fraudulent or duplicate claims, unnecessary tests and treatments, and other forms of waste;

c. Formalizing and adopting rules by which protection of patient information privacy would be implemented and assured;

d. Setting security standards through which the privacy protections would be implemented in technical and nontechnical methods and systems.

Most of the focus of the attention paid to this large and broadly-sweeping act has been on the changes it directs onto the first two of the three classes of entities:
1. **Covered Entities (CE):** plans, providers, and clearing house functions, each and all of which create, transmit, receive, and process a variety of electronic messages known collectively as “transactions,” which carry information, bill encoding, and other data elements (defined below). CE includes both institutions and individuals.

2. **Business Associates (BA):** a wide spectrum of business types that support the operations of CE in a variety of areas, including accounting, administration, nursing registries, and others, all of which involve handling the same sensitive information on behalf of the CE. This category includes subcontractors to BA’s as well as the BAs themselves.

3. **Couriers or Conduits:** this very narrowly defined category includes two basic types of service providers best regarded as a common carrier (Telephone Company) or a typical delivery service (United Parcel Service or United States Postal Service). This category is very sparingly applied, and those entities that qualify are all but completely exempt from these requirements.

The program that these entities must design and implement is based on risk management, that is, a program that quantitatively, qualitatively, or in combination:

a. Identifies and categorizes organization assets, and then prioritizes them by their relative importance to the operation in order to guide mitigation activities;

b. Determines the existence of vulnerabilities in those assets that, should the threats materialize, would allow, enable, or amplify the adverse impacts to the assets’ normal functioning;

c. Identifies and categorizes relevant threats to their assets (inclusive of information, systems, facilities, and personnel) that have a meaningful probability of occurrence and a measurably material adverse impact to the assets;

d. Evaluates the existence and effectiveness of countermeasures to prevent, minimize, or compensate for the impacts;

e. Selects and implements effective mitigations that have a positive cost-benefit ratio when compared to the value of the asset or the estimated overall cost of the compromise.

The requirements, called “Standards” that these entities must adhere to also fall into two classes:

1. **Required:** these often dictate “what” must be done, “why” it must be done, and are often self-describing as to the “how” it must be accomplished as well.

2. **Addressable:** those so designated also describe what must be accomplished, but allow the entity some latitude or creativity with regard to the form and manner of implementation used to achieve the intended goal. This quality enables the CE or BA to choose effective methods that fit the infrastructure or culture of the entity, rather than attempting to force-fit a predefined solution.

In many cases, there are “Implementation Specifications” that accompany the standards. Each of these identifies specific elements that must be addressed in order to achieve the goal of the standard. Both the Standards and the Specifications are described in greater detail later. Neither the Standards nor the Implementation Specifications are optional, but rather may be nonapplicable depending upon the type of entity or operation in question.

The information that these entities handle is known variously as “Individually Identifiable Health Information (IIHI)”; “Patient Identifiable Information (PII)”; and “Protected Health Information (PHI)”. The term “IIHI” is the most comprehensive of these and includes all types, elements, and forms of this information.

While there is indeed a difference in a legalistic sense between the definitions and the specific elements of each one, there is no effective difference between these type-labels from an operational or programmatic implementation perspective with regard to how they will be secured and protected. However, the most commonly used term is PHI, despite its strictest application is to this sensitive information being originated, handled, or otherwise manipulated by a Covered Entity, usually in electronic form. Consequently, for ease of understanding, this article will refer to them by the more common PHI.

Bearing the above in mind, all the standards and specifications reflected here are intended to be flexible and scalable so as to fit within the operations of nearly any CE or BA. They are intended to be technologically neutral, and as such to be widely implementable across the many structure and system types currently in use. Thus, these control elements will facilitate reasonable and sufficient protection in all three in which PHI will be found: expressed verbally, expressed on paper (by hand or machine printout), or in any way electronically (“at rest,” “in motion,” or in process).

It will be seen that there is a very noticeable emphasis throughout the law, its Code of Federal Regulations (CFRs) and rules that Management is actively involved and cognizant of all actions. This aligns with the companion thread of individual accountability. Within the body, HIPAA makes it very clear that the required documentation must be present and current, as well as being followed in practice. It also makes clear the necessity to ensure all parties to whom such guides apply are fully informed. As a capstone to these, the law states plainly that all parties will be held accountable for their behavior and adherence to the regulations. This reflects the
same approach to full disclosure as the Medical profession has had for decades through “informed consent.”

A HIPAA compliance program therefore is very “front-loaded,” as can be seen from the considerable amount of documentation required from which it is formed. The hazard in this is that a compliance audit will find that, while practice complies, the written guidance is often informal, out of date, or lacking entirely. While daily performance is clearly the proof of compliance, both are required for the program to conform, for a number of reasons:

a. Policy is the law of the organization, and is often driven by actual laws. The presence of policy illustrates awareness and enactment of that law within the organization.

b. The written policy makes clear what is required, and removes the potential to debate what would otherwise be verbal direction; hearsay, open to wide interpretation.

c. The written policy enables consistent and uniform enforcement along with metrics; again, removing the aspects of hearsay and general vagueness.

IMPLEMENTATION AND GUIDANCE

Taken directly, laws are difficult to implement as they give only indications of “what” result is expected when whatever modifications discernible from its text are accomplished, and “why” those to whom it applies are to do them. The institutional (the CE and BA) equivalent to a law is the policy.

Implementation instructions and supporting descriptive explanations therefore must be provided to enable affected parties to attain the desired results. For laws, these are given in the CFRs. For institutions, such instructions and supporting descriptions have their analogues in procedures, standards, and guidelines, each defined fully later.

This body of documentation enables compliant performance and sustains an ongoing program of maintenance of the compliant state. As such, they form a framework that serves as the primary basis of becoming and remaining compliant with both the law and the regulations that derive from it as may be written by the staff of the Department of Health and Human Services, the regulatory body that is the “owner” and enforcer of HIPAA. Getting compliant is often easier than remaining so over an extended period, but both are essential.

Adding somewhat to this difficulty is the “nonprescriptive” nature of HIPAA. It directs the impacted entities to perform a best-effort risk management approach to create and implement their privacy and security compliance programs. One result is that such a program at a given entity may vary greatly in its implemented form from that found at another entity. Another result is that the impacted entities are able to follow the guidance to achieve the compliance requirements in a manner consistent with the characteristics of the given entity. This approach enables compliance attainment across the widely varying landscape of entity-business types, and avoids the poor fit and even impedimentary outcomes of the traditional “one-size-fits-all” prescriptive approach found in other laws.

Thus, setting a program in place that facilitates evolutionary changes, as opposed to revolutionary changes, will add new task performance and modify existing practices with only minor disruption to workflow and will keep the additional administrative burden to an acceptable minimum. This “continuous process improvement” approach, versus the common “repetitive remediation and repair” approach, provides improved and more cost-effective outcomes over the long term in these programs.

STRUCTURE OF CONTROL CATEGORIES

The compliance requirements of HIPAA are expressed in terms of “Standards” and “Implementation Specifications.” The former is the directive regarding an area of coverage or a specific action (the “what” is to be complied with, and the “why” of the necessary objective), while the latter adds details regarding individual points requiring attention and action. To satisfy these, the structure of such a program has been broken down into four different and complementary controls categories:

1. Administrative: these are the paper-based documents that outline and guide performance and achievement of the goals, as described previously.

2. Physical: controls in this category are those that provide safety and security for facilities, rooms, and grounds, and guide performance of specific functions.

3. Technical: these are best thought of as implementations in hardware and software to enable security and privacy protections within computers, workstations, and networks, and specific steps regarding user behaviors.

4. Organizational: this category reflects the program of managing and controlling the contracts, records retention, and other processes that both CE and BA must perform periodically to ensure their attention to these requirements does not waver so that compliance is maintained long-term.

Individual control functions within each of these larger categories will vary depending upon what control
is selected and what desired effect is to be achieved. These functions are:

1. **Preventive**: a control that prevents undesired actions or results.
2. **Detective**: a control that alerts when an undesired or unauthorized action has been attempted (and may have succeeded).
3. **Corrective**: a control that enables reconfiguration of some feature or parameter to enable an authorized user to perform proper actions.
4. **Deterrent**: control that discourages some unwanted behavior.
5. **Recovery**: a control that enables restorative action to be taken to put a compromised system back into correct, usable condition.
6. **Compensating**: an approach that may use a variety of technical and nontechnical components to achieve the desired result without producing undesirable affects that a direct approach or control might cause.

Within each of the major categories there exists some example of each type of control function: some are technical, some are nontechnical, and some are process-based, while others are simply the consequence of a binary decision.

Throughout the body of the regulations appear the words “reasonable” and “appropriate.” The former means that, when correctly implemented and operated, the given measure does not create a situation of impaired operation, reduced care quality, undue administrative burden, excessive cost, technological fragility, excessive complexity, or other undesirable outcome. In other words, the concepts enable the CE or BA some latitude in seeking the remedy by emphasizing the achievement of the goal, and not a specific method to attain it. The latter refers to something “fit for use” such that when it is employed it is sufficient and correct in its application.

Compliance with HIPAA in the technology infrastructure of a CE or BA requires the assessment of conditions extant in that environment, an analysis of controls that are applicable to each use-case defined, and is accomplished through an informed selection process followed by a well-reasoned and skilled implementation of those controls and components chosen as fit for the given purpose.

Ultimately, a successful program will employ selected elements performing the desired functions from all categories. This program, as stated in the law itself, is intended to achieve security and privacy protections that are both effective and reasonable; that is, protective measures that accomplish the compliance requirement, in proportion to the quantified risks present and that ultimately do not interfere with the CE or BA’s ability to deliver quality patient care.

Thus, such a program must begin by assessing both the operational environment and the risks within it through the process of risk analysis, and an on-going program of risk management, which are two of the primary requirements laid out in the law. Such an analysis must assess both the technical and nontechnical aspects of the environment so that initial mitigating actions can be undertaken to establish compliant operations, and to enable the program of continuous awareness and management of risk to maintain the compliant state to become institutionalized.

The next sections will discuss and elaborate on the standards and implementations that are to be evaluated and employed to meet the objectives specified by the regulations. The sections will also define and discuss the terms “Required” and “Addressable” with regard to practical applications to meet HIPAA requirements.

**ADMINISTRATIVE CONTROLS FRAMEWORK**

This control category acts as a general repository of the documentation that will be used as the guidance for implementations intended to satisfy the specified requirements. In it are defined policies, procedures, responsibilities, and other programmatic elements for the various roles involved in achieving the ultimate compliance posture. Outlining the various processes, they fall into the following types:

1. **Policies**: spawned by the external regulations, these are the “laws” internal to the organization that state basis of “what” is to be complied with, and the “why” must it happen. Also stated in the policy is that any records not containing PHI are considered “operational” in nature and carry a 6-year retention requirement (health records containing PHI require a minimum of 7 years retention).

2. **Procedures**: these outline the “how-to” steps of the processes to accomplish the objectives described in the policies.

3. **Standards**: often defined as targets, these are products, services, methods, and configurations that are chosen as benchmarks or preferences that will be used or set to enable achievement of the compliance goal. In HIPAA, these are also the descriptions of what the CE or BA is directed to do to comply.

4. **Guidelines**: these may be best regarded as “preferred” practices to be employed in cases where implementing specific standards is not practicable. In cases where standards or specifications are termed “Addressable,” guidelines will outline considerations and approaches to be used to best meet the need, even though actual implementation outcomes might vary from case to case.
5. **Baselines:** these are defined minimums quantifying desired performance, benchmarks, or configuration from which variance will be measured.

In some cases, the stated standard may describe a process to be defined and implemented. Other cases may require a binary decision to be made to satisfy the requirement. The following outlines how in each case each of the above fits together with the others to provide a complete approach to each requirement and implementation specification.

The record types outlined here are regarded as “operational records”: that is, they constitute a body of records about IIHI describing its history, its evolution and so on. This body of records, however, does not itself contain any IIHI. As such, HIPAA specifies it is subject to a minimum 6-year retention period (states may independently lengthen this period), where patient records must be retained for a minimum of 7 years, unless lengthened by state law augmentation.

The following sections will outline each requirement, and detail an approach to each one, providing specific examples of how each may be successfully accomplished to secure the systems, data, and facilities in accordance with the regulatory requirement.

**Standard: Security Management Process (from 45 CFR § 164.308(a)(1))**

This standard states that a security management process must be defined and implemented to ensure that certain perpetual activities are in place, are clearly outlined and embodied in the five document types noted above, are performed periodically, and are supported and enforced by Management. The goal and intent of the standard is to ensure the CE or BA implement policies and procedures to prevent, detect, contain, and correct security violations. Within this standard are four Implementation Specifications:

**Specification—Risk analysis (required):** this specification means that a risk analysis process will be defined and adopted by the CE or BA, typically involving quantitative and qualitative methods, and will be employed consistently to evaluate asset-risk-threat relationships as they are found in the environment. “Assets” may be system, physical, human, or information in nature, but all must be evaluated in their operational context. The “Required” aspect means that a method of doing this must be chosen, validated, and consistently followed: it does not direct the precise method the entity will use. The process and methods used will be described in the document types noted above in sufficient detail that they can be competently employed by the appointed staff members, and the documentation generated by its performance will be comprised of

1. A comprehensive Risk Analysis report detailing and discussing all asset-risk-threat scenarios, the expected negative effect on the confidentiality, integrity, or availability of that asset, and the anticipated monetary value of the loss and associated recovery.
2. A Corrective Action Plan (CAP) that offers options and recommendations to: a) preventing the loss where and as possible and cost-effective; and b) describes contingency plan steps in the event of its loss to address the need to respond to incidents with or without a privacy breach.

**Specification—Risk management (required):** this particular specification is the primary element that will frame a program that will achieve the essential goal of the standard. This specification regards design and construction of processes that will enable the entity to manage its environment and operations such that risks are identified in a timely manner and mitigated. It implies a general risk identification and reduction program throughout the operation in administrative, physical, technical and, organizational areas, and requires this be a regular part of the operation to first achieve reasonable reductions and then to maintain that level. Meeting this requirement takes this form:

1. **Policy:** this would state that Management will implement and pursue a program of risk analysis in order to meet HIPAA requirements. It would specify the basic philosophy of risk management (risk-averse, risk-accepting, scenario specific), who shall be designated to perform these, the periodicity on which they will be performed, specify and define what metrics will be used, any sort of severity scale to be employed, decision criteria and acceptable variances to be employed.
2. **Standard:** this document would outline in sufficient detail what the chosen risk method is, its source and validity, and all necessary definitions and metrics.
3. **Procedure:** how the method is to be followed, step-by-step, and what items are to be used or examined. This would include calculations, evidence sources, interviews, and other items and actions to complete the process.
4. **Guidelines:** these would describe considerations, examples, and other recommendations for dealing with encountered situations and conditions that do not neatly fit models or assumptions.
5. **Baseline:** these would specify acceptable minimums and maximums for performance, variances, and similar boundaries and qualities.

As a general rule, standards and baselines would normally be included in the associated policy documents.
themselves, where procedures and guidelines would be attachments to them.

**Specification—Sanction policy (required):** this particular specification regards creating a new or modifying the organization’s existing general disciplinary policy to include the specific details of the types of infractions and their potential consequences under HIPAA. As such, it is derived directly from the law itself, and is more or less the essential points expressed unmodified in the entity’s policy style. Meeting this requirement takes this form:

1. **Policy:** Management would redraft the disciplinary policy to include the descriptions of the Tier I through Tier IV civil violations and possible consequences to the organization if such were committed and discovered (normally through periodic audit, complaints investigation, or other external exposing event). This would also include the same information for the Tier I through Tier III criminal violations and the related consequences to the individuals involved.

2. **Standard:** This describes a standard of behavior and as such would very likely be included in the policy document and require 100% adherence.

3. **Procedure:** This would describe how the entity will conduct routine audits of a technical (systems) and nontechnical nature, what evidence would be sought and used in doing so, and what it considers a qualifying violation. Typically this would also cover the results assessment process in order to determine appropriate courses of action.

4. **Guidelines:** These would typically take two forms. The first would be instructive guidance for the workforce members for avoiding violations and how to report them if found. The second would be for those performing the audits and would be derived from the Audit Protocols from the Department of Human Health and Services (DHHS) and the standard practices of the entity.

5. **Baseline:** As before, this would typically describe a 100% compliance posture.

**Specification—Information system activity review (required):** this particular specification regards creating a new or modifying the organization’s existing general disciplinary policy to include the specific details of the types of infractions and their potential consequences under HIPAA. As such, it is derived directly from the law itself, and is more or less the essential points expressed unmodified in the entity’s policy style. Meeting this requirement takes this form:

1. **Policy:** Management would redraft the disciplinary policy to include the descriptions of the Tier I through Tier IV civil violations and possible consequences to the organization if such were committed and discovered (normally through periodic audit, complaints investigation, or other external exposing event). This would also include the same information for the Tier I through Tier III criminal violations and the related consequences to the individuals involved.

2. **Standard:** This describes a standard of behavior and as such would very likely be included in the policy document and require 100% adherence.

3. **Procedure:** These describe the methodology to be used. As the law itself prescribes no specific method, this could be a derivation from the CoBIT standard, from JCAHO protocols, or from the issued protocols from DHHS itself (recommended source). The goal is to implement processes and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports, or a variety of other sources as appropriate.

4. **Guidelines:** For this specification, these would outline the specific types of informational evidence to be acquired, with guidance on how to extract, format, and interpret the contents.

5. **Baseline:** Most likely specified in the policy, the baseline would outline the periodicity, records selection modeling, and timelines.

**Standard: Assigned Security Responsibility (from 45 CFR § 164.308(a)(2))**

This standard mandates the appointment of a staff member who will be responsible for the development and implementation of the policies and procedures required to accomplish the program objectives: i.e., the achievement of compliance. This particular standard has no associated Implementation Specification; the member is appointed to act in the role (compliant) or not (noncompliant).

This is an example of a binary decision. The CE and the BA must each appoint someone, with the appropriate qualifications and experience, who will undertake these efforts to lay the groundwork for attaining the objectives. This would typically be a senior person with holding a Certified Information Systems Security Professional, a Certified Information Security Manager or other professional credential indicating they are technically qualified to perform this work. They must also be informed of and sensitive to the organization continuing to meet its operational objectives as well; in other words, they must work with Staff and Management to balance these potentially competing priorities and have the authority to perform this role. Often they will hold the title of Chief Information Security Officer (CISO).
To effectively act in this role, the CISO must gain a full understanding of the requirements, the operational issues, the culture, and find the balance among them to be successful. This requires a detailed approach in collaboration with the IT staff and representatives of Management and the User Community in order to facilitate acceptance and compliant performance of all parties. They must likewise appreciate the complementary nature of the controls in the technical and physical areas such that they are able to choose appropriate implementations that do not adversely impact business success.

**Standard: Workforce Security (from 45 CFR § 164.308(a)(3)(i))**

This standard requires that various policies and procedures be constructed and enforced to ensure that all workforce members are authorized access to PHI commensurate with their job requirements. It goes on to require preventive measures be put in place to protect against inappropriate or unauthorized access. In general, accomplishment of the intent of this standard requires a well-formed, documented access control policy and procedure to lay the foundation, and an Acceptable Use Policy and End-User Access Agreement (for each user to sign) to implement and enforce it.

This standard has three Implementation Specifications:

**Specification 1: Authorization or Supervision (Addressable)—**This is a straightforward requirement but an important one because it reflects the critical need for Management to be activity involved in the approval and monitoring of all workforce members accessing protected information. This represents a process type of requirement, considered addressable as it must conform to the culture of the entity even while it satisfies the requirement.

This involves the need for Management to review staff roles and take decisions about what access and what level of privilege is appropriate for each member in a given role. It also reinforces the fact that, ultimately, Management is accountable for such access and any deviations from policy or violations of such access or privileges by workforce members using their accounts. If Management delegates this responsibility, there must be a memorandum so noting on file, and they must still review the activity periodically themselves.

The process involves the specific steps:

1. Assessment of role and access levels and needs for it
2. Formal authorization, followed by provisioning activities

Proof of compliance would normally be established through the presence of and examination of audit reports accompanied by documented corrective actions and their results.

This process will also satisfy the “Access Authorization Requirement” defined in 164.308(b)(4), and the “Access Establishment and Modification” noted in 164.308(c)(4).

**Specification 2: Workforce clearance procedure (addressable)—**This requirement relates particularly to how each member is placed in a role and how their information system access is defined appropriately for that role. Background checks and other clearance steps would normally be completed through the Human Resources function.

The basic principles at work involve the members “Need to Know” and “Least Privilege.” These take the role and translate it into role definitions and access control rules for data that enable access to all pertinent systems and information but only to the lowest level possible. The role of “Nurse” would provide access to patient records but would exclude all data not defined as a part of the patient record. The same would be true of a “Staff Doc;” however the latter would likely differ in actual access to that of “Associate Doc” that might have access only to those patients they have been referred from their outside practices.

The roles and rules would be defined in Policy and implemented by provisioning Procedures. The Standards applied would describe the construction, aging, change intervals, and other specifics of passwords members are to use. Guidelines would be provided to all members to enable them to comply with the policies and construct proper passwords. All of these are addressable, in part because the current standards used by industry are continuously evolving and improving, and in part because each organization is operationally unique.
Specification 3: Workforce Termination Procedure (Addressable)—This requirement relates particularly to how each member will be processed out of the organization, and applies whether the separation is voluntary or involuntary. The primary objective is to ensure specific, procedural steps are routinely taken in order to reclaim all company property (access keys, tools, etc.), recover any information assets acquired by the workforce member, and to hold an exit interview during which the member should be reminded that HIPAA requirements to safeguard patient privacy remain in force following termination.

STANDARD: Information Access Management (from 45 CFR § 164.308(a)(3)(i))

This Standard requires the entity (CE or BA) to create a control framework that enables it to validate and authorize access to electronic PHI for any party requesting or claiming that such access is needed.

Specification: Isolation of healthcare clearinghouse (required)—This requirement addresses the need for clearly delineating access to information to: 1) avoid conflicts of interest (COI); 2) set a specific process in place to characterize access requirements by role; and 3) ensure that Management is directly and actively involved in the routine oversight of these processes. The latter two requirements are Addressable for the same reasons noted above.

The first of these implementation specifications (Required) regards a CE functioning in part as a Healthcare Clearinghouse (HCCH): an entity that acts to process nonstandard format covered transactions into the required standard form prior to submission for acceptance and adjudication. The COI element addresses the situation where a CE that may in the main be a provider organization, but contains a unit that performs HCCH activities, because such an arrangement without proper separation and controls enables the potential for the creation of fraudulent transactions.

In such CE, proper implementation requires two basic things: 1) identification of the HCCH component and creating an “arm’s length” legal separation between it and other units of the containing CE such that any input from them is subjected to processing in a fashion identical to input submitted from an outside CE with all associated controls; and 2) the creation of a role that creates full logical isolation for the HCCH and its workforce, and enforces all applicable controls to ensure full auditing capability to validate that this isolation is complete and verifiable.

Specification: Access authorization (addressable)—This requirement carries with it the need to construct the electronic data access control framework that entails establishing and enforcing the following elements:

1. Policy: Management prepares a statement that lays out the regulatory requirements, and drafts a policy that takes the form of an “Acceptable Use Policy.” This document describes the various allowed and disallowed behaviors that all authorized users must abide by when granted access to systems housing sensitive information. It would also include descriptions of how access requests would be validated, approving authorities, appropriate role creation or assignment, and disciplinary consequences for violations discovered during auditing. This document would ensure that workforce members are made aware of the following conditions of use (displayed in the required Login Banner):
   a. Users shall have no expectation of privacy, to include e-mail usage.
   b. That the system and its contents are corporate property and as such they will be auditing and monitored, even to include Law Enforcement access should circumstances warrant.
   c. That any unauthorized use may constitute a federal crime, which is under the jurisdiction of the FBI.
   d. That all information accessed is considered sensitive and is protected by rules of nondisclosure as well as state and federal regulations.

2. Standard: This describes a standard of behavior and as such would very likely be included in the policy document and require 100% adherence.

3. Procedure: These describe the validation methodology to be used, evidence required, and any necessary documentation. This would also apply in case of escalation, de-escalation, or other alterations in access types and levels.

4. Guidelines: If present, guidelines would normally recommend considerations that would modify access request evidence requirements, provide temporary access and levels when and if required, and how to handle violations.

5. Baseline: Typically not necessary in this case.

As an addressable requirement, this one recognizes the necessity to scale and adapt to the particular system architecture features used by the CE or BA, as there are many and they vary widely in the capabilities and sophistication. The objective is to configure the available features to meet the required details and performance, within the system’s capability envelope. In cases where certain aspects cannot be configured to precisely meet a requirement, compensating controls (usually closest approximation in configuration coupled with increased monitoring) must be designed and implemented. This situation may also result in unmitigated risk, which must be documented with a narrative describing how this risk will be monitored to prevent any unknown and adverse change in its character.
Specification: Access establishment and modification (addressable)—In practice this requirement is met through diligent performance of the above. It underscoring the emphasis mentioned earlier that Management should be directly involved in any material change in access levels and types granted workforce members or other authorized entities. It further requires that there should be an auditable trail of documentation to validate any change performed.

STANDARD: SECURITY AWARENESS AND TRAINING (FROM 45 CFR § 164.308(A)(5))

This standard includes four Addressable implementation specifications:

1. Security Reminders
2. Protection from Malicious Software
3. Login monitoring
4. Password Management

Successful implementation of this standard begins with a basic awareness briefing that must be delivered to all workforce members at all levels and of all types that will be handling PHI to set the baseline for the CE or BA by informing all members of the basic requirements for secure and proper handling of this sensitive information. Specific subgroups with particular roles should also receive training in topics pertinent to such roles. Following the establishment of such a baseline, ongoing training should be provided as an integral part of New Employee Orientation (NEO) delivered by HR. The CISO would participate with HR to set the topics and their coverage.

The four items listed above would be covered at sufficiently detailed levels to ensure the workforce is properly informed about the given issue, and that they are reminded periodically of the importance of adhering to policy: frequent enough but not so frequent or of a kind that they build up a “psychological callous” to the message.

“Protection from malicious software” would discuss, in layman’s terms computer viruses and other malware, how to recognize these threats, and the dos and don’ts (i.e., don’t open e-mails from unknown sources, do ensure your antivirus software is always running and up to date).

“Login Monitoring” is a briefing topic through which the CE or BA informs its staff that all computer activity is monitored and recorded. Though a potentially sensitive subject, all workforce members must be enlightened that this is constant and universal. In addition, the staff should likewise be informed that audit reports are generated from this system log and are reviewed regularly for anomalous or inappropriate activity.

In support of this policy, every CE and BA should have implemented a “Login Warning Banner” adapted from the basic text provided by the Department of Justice as a deterrent control—the first thing all staff see at login. In effect, it begins their awareness training by informing at every login of the conditions for its use. It should inform them of the following (an expansion of the above):

1. The system is a business asset to be used for business purposes only. As such, the organization reserves the right to periodically audit system or user activities to ensure that these resources are being used only for such purposes.
2. Users should have no expectation of privacy when using these information systems.
3. Logging in to the system gives the users’ consent to having their activity monitored and potentially recorded.
4. Any attempt to login by unauthorized users is a federal crime and therefore no such attempt should be made.
5. The information in this system contains sensitive and private elements and must never be disclosed by any means to any unauthorized party.
6. Users will exercise their assigned levels of access and privilege in the performance of the assigned roles, and should at no time attempt to perform unapproved activities that diverge from or exceed these levels.

STANDARD: SECURITY INCIDENT PROCEDURES (FROM 45 CFR § 164.308(A)(6))

This required standard has no implementation specifications associated with it, but is one of the more important compliance program elements.

With the very common condition that most CE or BA operations have live Internet connections that in some way interact with their business or PHI-handling systems, each has assumed the risk that this global and untrusted network can and will at some stage convey a threat agent or electronically-borne attack vector to their system and will thus cause a material and potentially devastating impact. Notwithstanding the fact that most, if not all have already implemented protective countermeasures against these agents and vectors, every CE and BA must have a proven plan to respond to these events and take every reasonable and possible action to contain and minimize the effects of them.

Guidance on how to undertake a program of Incident Response, Analysis, and Reporting was issued by Centers for Medicare & Medicaid Services (CMS) internally, and to its contractors in 2008 (Version 2.1).
The National Institute of Standards and Technology (NIST) has also published a guide on Security Incident Handling (Special Publication Series 800-61), which describes in sufficient detail the construction of a capability and steps to effectively prepare, identify, respond, contain, and recover from these adverse events, regardless of type. The CMS guide was derived from this, and both are applicable to either security or privacy compromise events.

For the CE or BA undertaking to construct a response team, it should begin with its risk assessment (RA) and a business impact analysis (BIA) to clearly identify areas where these agents are most likely to enter or arise, and assess the potential type and magnitude of such an event. This will permit focus on areas needing the greatest and most immediate attention; areas that when struck will impart the highest and most costly impact. At this stage, the entity must consider the skills and experience required by the prospective team members, whether it desires to create this capability internally or outsource it (the law makes no comment on either being preferred, only that the capability must be created and be effective).

Normally, the responses to be employed are characterized by scenarios, and the steps of response are defined appropriate to each context. Following this, the steps to perform are:

1. Prepare: this phase uses the RA and the BIA as guides to employ when selecting controls and countermeasures to offset areas of weakness, to strengthen it against compromise through procedures and technologies and to enhance its resilience, resistance, and recoverability.

2. Identification: using alert mechanisms, monitoring, auditing, and other detection methods, the entity must find and validate the seminal event indicators as early as possible. HIPAA considers the “day of discovery” of an event as Day 1, regardless of when the compromising agent now identified actually occurred.

3. Response: throughout the event, every person involved must keep a record of all steps taken and their outcomes. Chain of Custody must be observed by all at all times. Each type defined in reference to the type of incident or agent (malware, hack, internal, external, etc.), the response must be commensurate in type and effort to that agent, and should be proceduralized in steps:
   a. Investigation and Analysis (critical to determining the next course of action of response type)
   b. Containment (damage control activities)
   c. Eradication (clearing and verification activities)

4. Recovery and Restoration: These steps are vital to heal the compromised elements and restore normal (or as near to normal as possible) operation.

5. Review and reporting: Once the crisis has been reduced and normal operations resumed, the after-action review will be conducted to evaluate the process, the outcome, and next steps, which may include breach notification activities (must be performed as soon as possible, but not later than 60 after Day 1). This phase is vital to continuing to improve the quality of this capability.

Incidents are very costly, and are unavoidable over the long-term. These are made even more costly when associated with breaches of unsecured (unencrypted) PHI. Effective response is also often greatly impeded by ineffective investigation and analysis techniques.

However, these cost factors and management aspects must be compared to the negative impacts that will be suffered without this capability in place to prepare for and respond to these events, in addition to a failure to comply with the requirement. A business case will most often show that the offset is in favor of having the capability in place even without the requirement as the force behind having it.

**Standard: Contingency Planning (from 45 CFR § 164.308(a)(7))**

This requirement is intended to establish and implement policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. It is one of several requirements within HIPAA that addresses business continuity and disaster recovery planning activities. This particular entry has five implementation specifications within it. The NIST Guide (Special Publication 800-34) provides the basis for the CMS guidance on contingency planning and is itself an excellent guide to this topic.

**Specification: Data backup plan (required)—**The purpose of this requirement is to establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.

The practical implementation of this requirement is the composition of operational procedures to identify and categorize data based on type, frequency of change, and other parameters so that a schedule of backup processing is constructed and regularly performed. Most organizations have already performed this action, and make daily-use and archival backups. It makes no reference to business operations data, only to PHI and claims history. The regulations also take notice of whether the backups are made to disk or to tape, although the language seems to assume that the latter is the customary form.
HIPAA has added some significant details to this activity however in light of the sensitivity of the data involved:

- The first is that samples are pulled from selected backup runs, and test restores are performed. This action is to provide assurance that the backups can in fact be restored in usable form.
- The second (derived from the CMS guidance following the HITECH passage) is that backups should be encrypted if the system possesses the capability to do so. This renders the data “secured PHI” since the media is movable/removable and enables it to be moved safely offsite as “data in motion” as well.

**Specification: Disaster recovery plan (required)—**
The purpose of this requirement is to establish, implement, and periodically test plans and procedures to restore the information systems capability to an operative condition in the event of some magnitude of outage-causing event. Plans of this type address the needs of both business continuity and disaster recovery. In both cases, the plans developed are location and entity specific.

The continuity portion focuses on the business operations and directs planning and preparation actions to first, make the operation more resistant and resilient in the face of adverse events, and second, to create responses that will enable the business to restore operations to a minimum survival level as quickly as possible following the outage event.

The disaster recovery portion of the overall plan regards the event itself and directs focused, scenario-based activities to stabilize the circumstances, assess the damage, and set about to recover and restore operable IT services as quickly as possible through a variety of means and methods.

The requirement here is to ensure that an appropriate planning effort is conducted and that a viable, actionable plan is produced, tested, and implemented. The requirement includes annual testing and updating to ensure the plan stays current and relevant in the face of potential organizational or structural changes to the entity and its facilities. All tests must be documented and are auditable records.

**Specification: Emergency mode operations plan (required)—**The purpose of this requirement is to establish and implement procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode. This then is the very essence of the business continuity portion of the overall Disaster Recovery plan.

**Specification: Testing and revision procedures (addressable)—**The purpose of this requirement is to define and implement a process for the periodic testing and revising of the continuity and disaster recovery plans procedures. This activity requires that the CE or BA perform annual (at a minimum) testing of these plans and capture both the performance and results of the test. It also requires that the test type and its results be documented as auditable records, and subsequently be applied to modify the existing plan to ensure its continuing appropriateness and relevance to the operation.

A variety of methods are available for application: checklist, structured walk-through, simulation, parallel, and full interruption. While the regulation here is addressable in its formation and execution, the conduct of the test and the subsequent updating of the plans and procedures is not. The regulation does not require the entity assume the risk of the full interruption type test (this type can precipitate a major outage if preparations are inadequate), but it does require that whatever form the test takes, that the results are applied to proper effect when incorporated into the plan.

**Specification: Applications and data criticality analysis (addressable)—**This requirement is intended to assess the relative criticality of specific applications and data in support of other contingency plan components. The output from this process will produce required audit evidence documentation.

The conduct of this activity is required during a BIA to determine the character of the systems, applications, and associated data in order that a priority order can be established to facilitate the recovery effort. A NIST guide exists that can assist with performing this: Special Publication Series 800-60.

Though potentially tedious to perform, the output from its application will enable the CE or BA to determine which IT elements and data are of greatest importance to the operation so that a restoration order based on priority can be set to make the overall restoration more efficient. More importantly, the output from this process is often very revealing to Management by identifying previously unknown crucial areas of systems and data that have direct bearing on organizational survivability and possible exposure to data breach or unavailability, and the consequences to operations.

**Standard: Evaluation (from 45 CFR § 164.308(a) (8))**

This standard embodies the periodic (annual) reperformance of the original RA and addressing any changes in risk posture from existing sources, and any new risks that have become evident. This is required for both CE and BA entities.

This reperformance includes all the technical and nontechnical aspects, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic PHI, which
establishes the extent to which an entity’s security policies and procedures meet the compliance requirements then in force.

**Standard: Business associate contracts (from 45 CFR § 164.308(b)(1) and. 314)**

This standard specifies the drafting and execution of a business associate contract (BAC) that describes in detail all terms and conditions that the Covered Entity will expect the BA to perform. The BAC is thus a reflection of the BA’s duties and requirements under HIPAA to do all things necessary to perform its contractual obligations for services, as well as to perform (as the CE is required to do) to process and safeguard the PHI it will handle on that CE’s behalf.

The BAC also directs the BA to enforce the same conditions and requirements on any subcontractor it may engage to perform its duties in response to the primary BA’s contractual requirements to the CE.

Under the original legislation, it was assumed the BA would receive the BAC from the CE, and that the language would read as indicated above. Subsequent analysis proved that many BAs were operating without a BAC in force, never having gotten such from the CE. The remedy applied by the passage of HITECH was to formally require all BAs to be subject to the same privacy and security requirements already enforced upon CEs, and that the BA could originate with either party, so long as one existed and was enforced by the CE.

An additional change in the HIPAA definitions (45 CFR § 160.103) came in the form of a clarification through the Omnibus Rule issued by DHHS in January of 2013. This clarification stated that subcontractors to BAs are themselves BAs, and are therefore subject to all the same requirements historically accorded to both CE and BA, so long as the functions the subcontractor performs in its contractual duties supporting the BA, conform to the same criteria, as do those of the BA itself in support of the CE.

**Standard: Documentation (from 45 CFR § 164.316(a) and 170.210(d))**

The required standard in §164.316 embodies the directive to maintain as current the documentation prepared (as described above) and prescribes these specifications:

**Specification: Time limit (required)—**This requirement establishes the 6 year records retention cycle period for these operational (no contained PHI) records: from the date of their most recent retirement and replacement by a superseding version. There must be a policy setting this forth, accompanied by a procedure outlining the review, updating, and re-issuance process. All of these elements are auditable.

**Specification: Availability (required)**—This requirement directs that all persons involved in this maintenance process have access to all guidance in order to carry out their duties.

**Specification: Updates (required)**—This requirement directs that all documentation created in this program must be reviewed no less often than annually, or as circumstances or changes warrant, and that updates (as required) to them will be issued accordingly. It necessarily follows that all procedures affected by changes in policy must likewise be updated. All superseded versions then go into the retention program, and all new versions are reissued and covered with all affected parties in briefing sessions.

**Specification: Disclosure accounting (required)**—This requirement comes directly from HITECH, and directs that specific data elements (date, time, patient identification, user identification, and a description of the disclosure) must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR § 164.501.

This requirement has been changed to mandate that all electronic health record (EMR/EHR) software be capable by January 2014 of keeping records of any disclosures made beyond those made for treatment, payment, and healthcare operations (“TPO”) purposes. The Omnibus Rule also required that the default form of the record requested should be offered as electronic. Hardcopy versions would serve as the alternate form.

**PHYSICAL CONTROLS FRAMEWORK**

No program such as this can succeed without a complete program of guidance documentation properly implemented. If the Administrative controls framework forms the basis of a HIPAA compliance program, the Physical controls section of the requirements complements this as an implementation derived from it. This section of the regulation presents four Standards, and within them a total of ten Implementation Specifications.

The physical controls set forth in this section embody those determined by the regulatory authors as being those with the most relevant and important effect—positive if present, negative if absent—on overall program success in safeguarding PHI (in all forms) from compromise while enabling appropriate access and use. These choices then reflect the continuing emphasis on positive control and protection without creating undue hardship or excessive administrative burden on the CE or BA implementing them.
Standard: Facility Access Controls (from 45 CFR § 164.310(a))

The required standard in 164.316 embodies the directive to implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. The process reflected here is identical to the process used to enable system access, and emphasizes the same “need-to-know” and “least privilege” requirements on everyone to whom access is granted.

Thus reinforced, this general approach then becomes embedded within the organization’s methods and decision-making logic: grant access and level to all requiring it commensurate with their role and defined need. Restrictive but appropriate, such practices enable a general evolutionary systematic reduction in risk throughout the entity by contracting its exposure to both internal and external sources of risk while continuing to enable workforce performance and success.

This standard proscribes these specifications:

Specification: Contingency operations (addressable)—This requirement mandates that the CE or BA create and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan. This means that official members of the Continuity and Recovery teams are authorized to re-enter the facility (when deemed safe) and begin recovery and restoration operations.

This specification would describe site assessment and damage control measures to be used by the teams to evaluate whether reoccupation is advisable, criteria to apply regarding whether to activate the entity’s DR plan (or portion of it), what steps are to be followed to restore operations, and precautions to be employed to minimize further disruption and damage. These procedures describe marginal conditions that would dictate activating the offsite recovery capability in the event (regardless of cause) that reoccupation is infeasible. All of these elements are auditable through document examination and performance observation.

Specification: Facility security plan (addressable)—The plan itself is one typically found in most organizations, whether they are located in single or multitenant facilities. In that each organization’s circumstances will be unique, this element directs that policies and procedures be implemented to ensure the safeguarding of the location, its physical assets, the information and systems, and the workforce members from unauthorized physical access, tampering, theft, and potentially hazardous conditions.

Plans such as these will contain programmatic elements that address both safety and security concerns. They typically contain procedures for handling disruptions, vandalism, bomb threats, forcible invasion, environmental events (gas leaks, flooding, HAZMAT, etc.), fire and other nonnormal occurrences.

This plan would include elements that would describe any periodic testing of fire suppression and alarming systems, emergency power generation equipment, fire drills, emergency response drills with police, EMS and fire units in the area, mock disaster events, and other activities that provide assurance of adequacy of the procedures and readiness of the staff. All records of these activities must be retained for audit purposes and are subject to the 6-year retention requirement.

Specification: Access control and validation procedures (addressable)—Here again is a programmatic element that emphasizes the appropriateness of access requested and the necessity of Management’s involvement in its evaluation and approval. The process defined under this requirement is applicable to both workforce members (CE or BA) and to visitors. All aspects of these procedures would normally be covered in awareness briefings and during NEO.

Specification: Maintenance records (addressable)—This requirement relates to those specific records generated through the installation, maintenance, repair, and decommissioning of any system that has anything to do with facility or data center safety and security. These records are also subject to the 6-year retention period to maintain congruence with similar operational records, and to map to the 7-year retention cycle for PHI records.

While most organizations are already retaining such records for purely business reasons, the HIPAA requirement reflects an appreciation of the impact of the physical upon the technological. Many cases of disasters, whether accidental or intentionally caused, can be attributed to poor maintenance practices, or to tampering and sabotage. These records may contribute important information to investigations of facility or systems events and breaches, and as such they constitute a vital part of the overall security program.

Standards: Workstation Use (164.310(b)) and Workstation Security (164.310(c))

These two required standards together lay out the principles behind how workstations will be deployed and used through the facility. They also contain environmental elements complementary to the “Acceptable Use Policy” that guide user behavior.

The Workstation Use standard requires drafting policies and procedures that specify the proper functions to be performed, the manner in which those functions are
to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

The practical implementation result is a general directive stating that workstations in a given area, such as Patient Care, Administration, or the ER, are to be used solely for the normal functions of that area. The technical implementation of this policy would involve defined security policies on servers and hosts that enable users to sign into the systems and perform their normal role in their home area, but not in others.

The **Workstation Security** standard requires that physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users. Implementation of this standard typically involves the use of physical anti-theft measures, tamper detection devices and seals, and various forms of “lock-downs” such as cable locks (normally for laptops), locking cabinetry, and other methods.

The combination of these two standards will produce an environment where the workstations are:

1. Configured such that only functions of a given area can be performed on the workstation, and then only by authorized workforce members;
2. Arranged in such a manner that will allow them to be used by authorized uses, while making it difficult or obvious should an unauthorized person attempt to do so;
3. Positioned such that any person in the area cannot observe PHI displayed on the screen except from the user’s primary position;
4. Secured by such cabinets, locking devices, and detection mechanisms possibly including CCTV.

The point of these standards is to restrict system user activities to appropriate areas in order to minimize the incidental disclosure of PHI to the workforce within the facility, and to reasonably eliminate the opportunities for unauthorized parties to observe (without being obvious in the attempt) PHI displayed on computer screens.

**Standards: Device and Media Controls (164.310(d))**

This standard regards the use of any and all media and devices that may or will hold PHI of any kind. These devices are typically laptops, removable storage media (USB memory, CD, DVD, floppy disc, tape, and similar media), mobile phones, and tablets such as IPad, Droids, and their variants. Also included but often overlooked are the storage devices found within copiers and facsimile machines. Within the standard are four implementation specifications.

The first two specifications reflect an awareness that using such removable or transportable media raises high the risk that the loss of such a device, whether memory only or an actual computing device, will allow PHI to become exposed under uncontrolled, unauthorized condition and thus result in a breach, at a minimum. As can be gleaned from many news sources, such events are quite common and many thousands of records are compromised in this way annually. Consequently, these two required specifications are intended to effectively address these concerns.

The HITECH Amendment and rules guidance from DHHS-CMS adds important definition to these specifications also. No particular mention was made in the original legislation of how this data was to be protected; meaning that no specific discussion regarding the use of encryption technology was presented. Laws normally attempt to remain technologically neutral, and in 1996 these technologies were not as widespread, as low-cost, or as conveniently usable as they have become since.

The HITECH Amendment added the language that defined “secure” PHI: PHI that had been rendered “unusable, unreadable, or indecipherable to an unauthorized party” through the employment of a suitably sophisticated technological transformational method.

It further included that PHI had to receive such protection whether “at rest” (in storage, not in direct use), or “in motion” (in transmission through transport or tunneling methods). Rules issued by DHHS in August of 2009 following HITECH’s passage in February further clarified this, and stated that encryption technology, compliant with NIST proscribed standards, would in fact be required. This was further reinforced and clarified by the Omnibus Rule issued in 2013.

These rules specified algorithmic systems using components of cipher strength at least equivalent to AES-128 (minimum) for crypto-processing (confidentiality assurance), and MD5-128 (minimum) for hash-processing (integrity assurance). Evidence indicates that AES-256 and SHA (160/384 bit) are in more common usage as they provide greater protective strength and longer survivability against attack or when stored.

**Specification: Disposal (required)—**This requirement directs that when an entity elects to dispose of a particular device it must use a method that provides very high assurance that any reasonable attempt to reclaim the information previously stored on the device will be unsuccessful. Prior to taking this irreversible step, however, there exists the requirement to ensure that the data on such devices has been accounted for within the official records so that it is not lost to the authorized users and patients.

The law does not prevent an entity using an outside contracted service for the purpose, and such providers are commonly engaged. Doing so involves executing a services contract, inclusive of a Business Associate
Agreement/Addendum since the contractor and its personnel may well come into direct contact with PHI when performing their services. Such contracts normally cover the destruction processing of paper and electronic media. All processing is done onsite and Certificates of Destruction are to be provided before the contractor departs.

**Specification: Media re-use (required)**—This requirement directs that when an entity elects to re-use a particular device it must use a method that provides very high assurance that any reasonable attempt to reclaim the information previously stored on the device will be unsuccessful. Prior to taking this irreversible step, however, there exists the requirement to ensure that the data on such devices has been accounted for within the official records so that it is not lost to the authorized users and patients.

No mention is made that the final disposition must be destruction; the final disposition could be redeployment within the organization or an external donation of a computing device. Given that these options are equally possible, the CE or BA is expected to judge exposure potential and take appropriately strong, assured methods to reasonably ensure that no exposure (i.e., breach) can result.

Achieving this result can be done internally so long as the entity selects appropriate effective physical and logical means of destroying the information contained on the media. These methods would include (separately or in combination) binary over-writing, complete format (low-level or multiple passes), or strong magnetic erasure (degaussing). Actual physical destruction will provide positive assurance as well, but obviously renders the media nonreusable.

One source of guidance on methods acceptable for use would be the Department of Defense Guide known as the “National Industrial Security Program Operations Manual (DoDM 5220.22M),” which prescribes rules for both clearing (applicable for internal re-use) and sanitization (for media used externally). This guide is publicly available, but an extract of it and the specific methods described is provided in Appendix A.

**Specification: Accountability (addressable)**—This specification directs that an inventory tracking system be designed and implemented that: 1) identifies the device or media and labels it in some way (if feasible); 2) monitors its movements regularly; and 3) assigns a workforce member responsibility for that device. Most organizations of all types already have in place such a system, and continuously monitor device assignments and movement, as would be found when devices are installed, relocated within facilities, or decommissioned.

What makes the healthcare setting unique, however, is that the need of movement of data onto removable storage (beyond routine backups) would be a rare occurrence. Typically this type of PHI movement would not be permitted as such data is not used outside of a CE or BA facility. While certainly there would be exceptions to this, the standard policy for such actions would be a preventive control placed on USB ports and CD/DVD drives rendering them as Read Only devices or disabling their use for memory media entirely. Such action would not affect the use of headphones, webcams, or other nonmemory devices.

**Specification: Data backup and storage (addressable)**—This specification directs that whenever devices possessing local storage (harddrives) and are slated to be relocated or possibly decommissioned, that a backup be taken of the drive to ensure no data is lost.

The manner by which this is performed is not described in the rules, but could take the form of a remote backup done over its network connection, or a local backup performed using a portable backup drive (tape or disk). If the CE or BA employs the use of diskless workstations known as “Thin Clients,” no backup would be required as there is no permanent local storage of any kind.

**TECHNICAL CONTROLS FRAMEWORK**

The Technical Controls standards and specifications of the HIPAA/HITECH regulations outline areas of the IT infrastructure of particular importance and impact on the security and privacy of PHI.

Many things could be said to be at the heart of a HIPAA compliance program: the transaction automation, the privacy controls, or improved insurance portability. While good choices, none of them work as intended if the secure electronic information formats and processing requirements that underpin them are not effectively addressed. Thus it is to complete the protective envelope surrounding this sensitive information that the Technology Standards must be selected and implemented.

The technical controls described in this section are commonly accepted and used in most sectors of the American economy. While not an exhaustive set of controls, the ones proscribed by the regulations present a minimum set that will implement a cost-effective program that safeguards against the most commonly occurring threats that produce the highest amount of losses and privacy compromises of PHI. As one of the seventeen sectors identified as Critical Infrastructure by the Department of Homeland Security (DHS), the directive to adopt these controls brings healthcare into alignment with all other sectors, and with American commerce generally.

**Standard: Access control (from 45 CFR § 164.312(a))**

This standard, which contains five specifications, requires that a CE or BA implement technical policies
and procedures that will provide protection for electronic PHI and the systems housing it so that only authorized individuals, systems, programs, and other external entities are allowed access to it, regardless of the means of such access.

Implemented through the specifications, this standard ensures that Management is actively and directly involved in the details and oversight of validating access requests, actions taken when anomalous or unauthorized actions appear on audit reports. Ultimately these elements create a program of access protections that is designed, implemented, and operated appropriately to achieve the overall objective of assuring only authorized entities can access the information, only through authorized means, and then perform only authorized actions on that information.

**Specification: Unique user identification (required)—** A straightforward requirement, this specification directs that all authorized users be assigned a login identifier that is uniquely theirs. Though already a very common practice in many organizations, the nature of healthcare is such that systems may be built and deployed that do not carry this capability (if they are old enough). They may also enable the use of generic or group logins. Virtually no system sold today omits the capability to assign and monitor the individually assigned user login, but many still allow the creation and use of the generic types.

The fundamental principle here is “individual identifiability and accountability.” As in all other areas of these regulations, all entities having access to PHI must have a valid need-to-know, and the law enforces accountability on every individual and entity commensurate with such access. To make this possible, the system must be able to clearly and precisely identify and track each user or entity and their actions. Otherwise accountability and thus disciplinary action is unenforceable, and the sanctions policy or legal action all but pointless.

While there is not particular required format for the identifiers themselves, this policy will contain the specifications of their associated validating credentials:

1. **Type I Authenticators—something the user “knows”:** a password or PIN code.
   a. Complexity and content (length, mixed case, inclusion of numbers and special characters)
   b. Normal expiration periods
   c. History-generations precluding re-use
   d. Pattern prevention rules
   e. Dictionaries of denied words and combinations
   f. Minimum effective life, maximum usage period

2. **Type II Authenticators—something the user “has”:** a token device or card-key.
   a. A badge-card that also functions as a system access key by embedding credential-validation coding
   b. A token device that generates a one-time use challenge-response code in either synchronous (time driven) or asynchronous (event driven) mode

3. **Type III Authenticators—something a user “is or does”:** a biometric marker or action.
   a. Any one of a number of biometric traits that in real-time use are matched to a stored template. Examples include fingerprints, retina blood-vessel patterns, iris color/reflectivity patterns, or other passive characteristics.
   b. Any one of specific actions performed by the user during real-time authentication: spoken phrase voice prints, typing actions, or other user-unique actions.

Current regulatory requirements specify only Type I Authenticators as only these are built into virtually every computing environment, and as such require no additional software to provide the specified security features. If, however, the RA of the CE or the BA should indicate a type or level of threat that is unacceptable in this aspect of the system in use, the entity would be expected to evaluate this situation and develop a countermeasure for it (though not necessarily requiring the addition of Type II or III Authenticators). As no entity would be compensated by government funding to meet this additional risk, the actual solution deployed would be the most cost-effective possible, regardless of the technological solution chosen.

The audit records produced from this requirement are derived from the raw system logs and capture for all user activity:

1. Login/logout (data, time, originating address, and possibly other attributes)
2. Password change
3. Password mis-entry
4. Username suspension due to mis-entry or other reason (i.e., termination)
5. Change of privilege level (requires paper-trail authorizing this)
6. Transaction and file manipulation activities
7. Errors, violations, or other anomalies appearing during user sessions

The frequency of generation and review is described in the regulations as “periodic,” leaving it to the entities to define it precisely. This information is most usable and revealing when obtained daily, though weekly may be often enough for smaller, less active entities. Any less often and the information mass may be too great to evaluate in a meaningfully short period of time (more than a full day), or may miss certain activities. The raw logs do not have a records retention requirement on
them, but the extracted reports are operational records that are under the 6-year retention rule.

**Specification: Emergency Access Procedure (Required)**—A straightforward requirement, this specification directs that an all-powerful, nonsuspendable administrator is to create, the sole purpose of which is to enable an authorized administrator access to a compromised system to perform recovery activities, while ensuring that protection of the resident PHI will continue uninterrupted. The pre-packaged “Admin” login is often configured for this use.

The implementation of this requirement is a procedure involving at least three staff members: an administrator, a member of Management and a selected other member of the workforce. This process applies the principle of Separation of Duties-Dual Control to ensure no inappropriate use is made of this access:

1. Administrator: has the technical skill to use the username, but cannot access it as it is in the custody of the second workforce member and access to it must be approved by Management each time
2. Second workforce member: is the keeper of the username, but does not possess the technical skill to make any use of it
3. Management: must personally approve the username’s use every time it is required, review the transcript of all actions it is used to perform while out, and must sign off when it is refreshed and replaced in storage

All those involved in this process are formally assigned and are individually accountable for all actions taken during its invocation. All records generated through this are required to be retained as auditable for the 6-year period.

**Specification: Automatic logoff (addressable)**—This specification directs that either a full system logoff/logout is forced by the system’s security settings, or if this feature does not exist, that an acceptable alternative is for the system to force a screensaver to activate: in either case the feature is to activate after a preset time interval of user inactivity expires.

It is a normal part of Acceptable Use or Password policies as mandatory that users are to never leave their workstation sessions logged on if they step away from it for any length of time (an obvious exposure to misuse by another). This particular feature also ensures that a session times-out due to inactivity even if the user is present. The regulation originally required a full, forced logout, but Microsoft systems did not and do not support this. The HITECH amendment modified the requirement to allow the use of password-protected screensavers as an alternative. No specification was made as to the expiration period length (most use the system default of 30 minutes), but universal enforcement of the feature and the chosen duration are required (validated by technical compliance systems audit).

**Specification: Encryption and decryption (addressable)**—The origin specification from HIPAA [(164.312. (a)(iv)] required only that a suitable method to encrypt and decrypt PHI was found and implemented. While certainly a vital part of the over security program, no mention was made as the type or strength of the cipher to be employed to accomplish this. As with all addressable requirements, the law left the selection process to the CE or BA, so long as it was done, universally deployed on PHI-containing volumes and repositories, and that its use was consistent and of reasonably sufficient strength.

**Specification: Encryption and decryption (required)**—This added specification from HITECH [170.210(a)] extended the original and set strength and performance minimums for qualifying technologies and products considered for use. The HITECH version stated that:

1. Encryption and decryption operations were to use a symmetric (secret) key cipher 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit key strength. (This describes the Advance Encryption Standard (AES) in everything but name.)
2. Operations for key or information exchange require that an encrypted and integrity protected link must be implemented.

In the case of point b, this describes a public key (PKI) exchange involving the use of encryption for content confidentiality (symmetric keys themselves or PHI) and hashing for content integrity assurance. This applies equally to tunneling at setup or in normal use, or to message (transport mode) communications involving data “in motion,” whether actual PHI or cryptographic materials.

**Standard: Audit Controls (from 45 CFR § 164.312(b))**

This standard requires that a CE or BA implement technical policies and procedures that will enable a detailed and thorough examination of the logs and records produced by a system housing or processing PHI in order to make an accurate determination about the: 1) correct performance of the system such that information integrity is assured; 2) that authorized user activity can be shown in sufficient detail to determine policy compliance (or its lack); and 3) to provide supporting formation validating the overall management of the system such that these traits are observed and maintained through continuous and diligent performance of these processes.

**Specification: Audit controls (required)**—No additional detail is added by the original specification [(164.312(b)) except to restate the standard itself.
The specification for audit controls added by HITECH added a lot of detail to the standard, now requiring that the system log (from which audit reports are extracted) must record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, deleted, or printed; and an indication of which action(s) occurred must also be recorded.

There is no indication, even in the added details from HITECH, if there is a particular audit protocol to be employed. There is the Control Objectives for IT (CoBIT) standard that is widespread use, but it does not focus on healthcare systems or PHI. There is also the ISO 27000 series of security and audit standards, but this course is valid only if the ISO itself has been implemented and validated as having met HIPAA requirements. (Despite its globally recognized quality as a security framework, there is no mandate or reference within the regulations or CFR’s regarding its use).

The Office of Civil Rights (DHHS-OCR) has itself issued audit protocols for both privacy and security, and each Privacy Officer and Security Officer for each CE or BA should evaluate these as the applicable metrics to certify their own performance and preparedness for an official audit, or readiness for a complaints investigation.

**Standard: Integrity (from 45 CFR § 164.312(c))**

This addressable standard requires that a CE or BA implement policies and procedures that will direct selection and implementation of technical mechanisms that will protect electronic protected health information from improper alteration or destruction. There are no additional specifications for this standard.

Typical implementations for this standard involve the application of protective mechanisms that prevent editing or deletion of files even by those granted access to them. Coresident with these access controls are often integrity assurance mechanisms that record all changes, both authorized and unauthorized. Such mechanisms typically alert the file owners of attempts but do not act preventatively.

There will often be a variable level of detail these detection records provide as well: sometimes to the file level and other times to the field level. The regulations do not make clear which is preferable, but more detail is preferable to less, within reason.

**Standard: Person or Entity Authentication (from 45 CFR § 164.312(d))**

This standard requires that any entity, whether person or organization, granted access or to be provided any PHI be positively identified. This means that a combination of electronic and procedural controls must be implemented to: 1) first establish the entity’s need to know and authorization for acquiring the information; and 2) re-verify that the same entity is the intended recipient each time before a transmission of PHI is made. The controls employed must include provisions for transmission of PHI whether through a network, via facsimile, or mail.

**Standard: Transmission Security (from 45 CFR § 164.312(e) and 170.210(C))**

This standard requires that any form of PHI transmission must be protected against violations of its confidentiality and its integrity. The transmission types include tunneling (VPN), transport (message-based or e-mail), and facsimile.

**Specification: Integrity controls (addressable)** — The method used here would typically employ hashing as the assurance mechanism for detection of any alterations while in transit.

**Specification: Encryption (required)** — Specifies that a hashing algorithm of 160 bit strength or greater be used as the integrity assurance mechanism (equivalent to or greater than the Secure Hash Algorithm (SHA) certified by NIST.)

**Specification: Encryption (addressable)** — Added by HITECH and clarified by rules from OCR, this indicates that symmetric encryption at a minimum 128 bit strength must be used to sufficiently protect the confidentiality of PHI in transit regardless of transmission method.

**THE OMNIBUS RULE**

This was issued in January 2013 and extends the original HIPAA law and it’s HITECH Amendment. Rules provide clarification and refinement to the interpretation of the law to facilitate better understanding and implementation of the regulations.

Of the 64 total entries addressed by the Omnibus Rule, a careful analysis shows that only eight of these are in fact changes to the original legislation. Of these eight, two concern the breach notification process, three affect the patient’s ability to opt-out of various activities, and one deals with the clarification of a subcontractor (to a BA) as being a BA itself.

With respect to impact on the information systems function in particular, Omnibus has little if any direct effect. All indirect effects have already been noted above.
BIBLIOGRAPHY

5. The HITECH Act of 2009, (ARRA, Division A, Title XIII, Subpart D, and Division B, Title IV).

HIPAA: Health Insurance Portability and Accountability Act