PHYSICIANS’ GUIDE TO COMPLYING WITH THE
HIPAA/HITECH SECURITY RULE

I. HIPAA/HITECH

As part of the Health Insurance Portability and Accountability Act (HIPAA), Congress enacted measures to protect the privacy and security of an individual’s health-related information. Effective February 17, 2010, HIPAA has been amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), which strengthens and expands the protections required by HIPAA.

A. HIPAA/HITECH has three main Rules:

1. The Privacy Rule
   - applies to electronic, written, and oral “protected health information” (“PHI”)\(^1\)
   - tells you if, when, and how PHI may be used and disclosed

2. The Security Rule 45 C.F.R. §164.302 to 318
   - applies to electronic PHI (“e-PHI”)\(^2\)
   - sets standards for making sure that e-PHI is secure and available when needed

3. The Transaction Rule
   - addresses technical aspects of the electronic health care transaction process
   - requires the use of standardized formats whenever health care transactions, such as claims, are sent or received electronically

B. This is a guide for physician practices on complying with the Security Rule:

The following information is intended to give you an overview of the HIPAA Security Rule and how to comply with it. Complying with the HIPAA/HITECH rules is important. Violation of the Security Rule may result in civil or even criminal sanctions (see Section VII).

---

\(^1\) PHI is “individually identifiable health information” that is transmitted or maintained in any form or medium. Individually identifiable health information is PHI that either identifies the individual or that can be used to identify the individual. Health information is any information in any form (oral, written, electronic) that is created or used by health care professionals or health care entities.

\(^2\) E-PHI is PHI that is transmitted or maintained in any electronic medium.
II. THE HIPAA SECURITY RULE

A. The Security Rule generally requires you to:

1. ensure the “confidentiality, integrity, and availability” of all e-PHI that you create, receive, maintain, or transmit;

2. protect against any reasonably anticipated, impermissible threats or hazards to the security or the integrity of e-PHI and impermissible uses of disclosures of e-PHI; and

3. ensure compliance with the Security Rule by members of your workforce.

B. The Security Rule is organized into 3 groups of “Standards” with “Implementation Specifications” for each Standard:

1. Administrative Safeguards

2. Physical Safeguards

3. Technical Safeguards

The Standards set the requirements that you must meet to keep e-PHI confidential and secure; the Implementation Specifications provide details on how to comply with the Standards.

C. The Security Rule generally applies only to e-PHI:

In general, the Security Rule applies when a physician or someone acting on behalf of a physician, such as a billing service, transmits or maintains e-PHI in connection with a transaction specified by the Rule. Once application of the Security Rule is triggered, the Security Rule then applies to all e-PHI within the practice.

1. The Security Rule applies to “covered entities,” namely:
   - health care providers, such as physicians
   - health plans
   - health care clearinghouses

2. HITECH makes the Security Rule applicable to Business Associates, too.

---

3Health care clearinghouse is a public or private entity that: (a) converts or assists with the process of converting health information into standardized HIPAA-compliant data or a standard transaction; and/or (b) receives a standard transaction and converts or assists with the process of converting that standard transaction back into a non-standard format or non-standard data for the receiving entity.
3. The Security Rule applies **only to e-PHI**:

- The Privacy Rule applies to all PHI, but the Security Rule applies only to e-PHI.

- E-PHI is PHI that is transmitted or maintained in electronic media. Paper PHI is not covered by the Security Rule. **Electronic transmission** includes the Internet, extranets (using Internet technology to link a business with information only accessible to collaborating parties), dial-up lines, computer-generated faxes (but not traditional paper-to-paper faxes), private networks, and e-PHI that is physically moved from one location to another using magnetic tape, disk or compact disc media.

4. The Security Rule applies to “standard transactions”.

Like the Privacy Rule, the Security Rule applies when a covered entity maintains or transmits PHI in electronic form in connection with a “standard transaction.” If you engage in any of the following **standard electronic transactions** specified in the Security Rule, the Security Rule applies to you:

- health care claims
- healthcare payment and remittance advice
- health care claim status, enrollment or disenrollment in a health plan
- coordination of benefits
- eligibility for a health plan
- health plan premium payments
- referral certification and authorization
- first report of injury
- health claims attachments

III. **RISK ANALYSIS: THE FIRST STEP IN SECURITY RULE COMPLIANCE**

Just as you must have written policies and procedures as part of your Privacy Rule compliance, you must also have written polices and procedures as part of your Security Rule compliance.

But before you prepare your written policies and procedures, the Security Rule requires that you conduct a **risk analysis**.

As with other requirements of the Security Rule, **there is no one-size-fits all blueprint for conducting a risk analysis.** Rather, you must evaluate risks and vulnerabilities in your particular situation and then implement security measures that are reasonable and appropriate for your practice to protect against reasonably anticipated threats or hazards.
to the security or integrity of all e-PHI that your practice creates, receives, maintains or transmits.

In other words, Security Rule compliance is a process tailored to your particular situation, and risk analysis is the first step in that process. Methods of conducting this analysis will vary depending on the size, complexity, and capabilities of each practice. Whatever methodology you choose must, however, accomplish the objectives of the Security Rule.

A. General requirements and objectives of Risk Analysis

1. You must conduct an “accurate and thorough assessment” of the potential “risks” and “vulnerabilities” to the “confidentiality, integrity, and availability” of your e-PHI. (You will find definitions of these, and other key terms below in subsection C.)

2. Make a written record of everything you do as part of your risk analysis. It is also a good idea to record the names of the people who perform the risk analysis and the dates on which the various things were done.

3. To help you identify potential issues begin by identifying:
   - all e-PHI that you create, receive, maintain, or transmit
   - the external sources of e-PHI (e.g., vendors or consultants who create, receive, maintain or transmit e-PHI for you)
   - the “threats” to information systems that contain e-PHI

4. The outcome of your risk analysis is a critical factor in assessing whether an Implementation Specification or an equivalent measure is reasonable and appropriate. (See Section IV.D. below for details.)

5. The information you get from your risk analysis will be used, for example, in designing and implementing policies and procedures:
   - for appropriate personnel screening
   - on what data to backup and how
   - on whether and how to use encryption
   - on what data must be authenticated in particular situations to protect data integrity
   - on how to protect e-PHI transmissions
B. Required Elements of a Risk Analysis

There are various ways to perform a risk analysis; the Security Rule does not prescribe any single method that will guarantee compliance. But regardless of what method you use, your risk analysis must incorporate the following elements:

1. **Data Collection**

   You must identify where the e-PHI is stored, received, maintained or transmitted.

   - This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards and other storage devices, personal digital assistants, transmission media, or portable electronic media. “Electronic media” includes a single workstation as well as complex networks connected between multiple locations. Your risk analysis should take into account all your e-PHI, regardless of the particular electronic medium in which it is created, received, maintained, or transmitted or the source or location of the e-PHI.

   - Gather relevant data by reviewing past and existing projects, conducting interviews, reviewing documents, or using other data gathering techniques. Document all the data on e-PHI that you collect using these methods.

2. **Identify and Document Potential Threats and Vulnerabilities**

   You must identify and assess the potential “threats” and “vulnerabilities” to the confidentiality, availability, and integrity of all the e-PHI that your practice creates, receives, maintains, or transmits.

   - You must identify and document reasonably anticipated “threats” to e-PHI. You may have threats that are unique to the circumstances of your environment, for example a high likelihood of break-ins in your neighborhood.

   - You must also identify and document “vulnerabilities” which, if triggered by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.

3. **Assess Current Security Measures**

   You must then assess and document:

   - the security measures you currently use to safeguard e-PHI;
• whether security measures required by the Security Rule are already in place, and

• whether your current security measures are configured and used properly.

Note that the security measures implemented to reduce risk will vary among practices. For example, small practices tend to have more control within their environment, with fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions about how to safeguard e-PHI. As a result, the security measures necessary to reduce the likelihood of risk to the confidentiality, availability, and integrity of e-PHI in a small practice may differ from those that are appropriate in large practices.4

4. **Determine What Threats Are “Reasonably Anticipated”**

Since you are required to protect against threats to e-PHI that are “reasonably anticipated,” you must determine what threats are “reasonably anticipated” in your practice by:

• assessing the probability of potential risks to e-PHI; and

• documenting all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability, and integrity of your e-PHI.

The results of this assessment, combined with the initial list of threats, will help you determine which threats are “reasonably anticipated.” Those are the threats that you must protect against through appropriate security measures.

5. **Determine the “Criticality” of the Risks**

You must also assess the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. Consider the magnitude of the potential impact resulting from a threat that triggers a specific vulnerability. You may use either a qualitative or quantitative method or a combination of the two methods to measure the impact.

---

4 For more information on methods smaller entities might use to comply with the Security Rule, see #7 in the CMS Security Series papers, entitled “Implementation for the Small Provider” at [http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf).
Document all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of your e-PHI.

6. **Determine the Level of Risk**

You must assign risk levels for all threat and vulnerability combinations that you identified in your risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

Document the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

7. **Finalize Documentation**

You must document your risk analysis. No specific format is required. Be sure to keep your documentation. It is also a good idea to list the names of the personnel who participated in the risk analysis and the dates on which various tasks were performed.

8. **Periodic Review and Updates to the Risk Assessment**

Because the Security Rule requires you to update and document your security measures “as needed,” your risk analysis process should be ongoing and continuous so that you can identify when updates are needed.

The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency will vary. Some practices may need to perform these processes annually, others bi-annually, and still others only every 2 or 3 years, depending on circumstances of their environment.

Certainly a risk analysis should be performed as new technologies and business operations are planned. For example, if you experience a security incident, or if you have a change in ownership, a turnover in key staff or management, or if you are planning to acquire new technology, the potential risk should be analyzed to ensure that e-PHI is reasonably and appropriately protected. Should you determine that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, you must determine what additional security measures are needed.
As part of your documentation, you might create matrices similar to these:

### Likelihood of Occurrence Levels

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Unlikely ever to occur</td>
</tr>
<tr>
<td>Very Low</td>
<td>Likely to occur two/three times every five years</td>
</tr>
<tr>
<td>Low</td>
<td>Likely to occur once every year or less</td>
</tr>
<tr>
<td>Medium</td>
<td>Likely to occur once every six months or less</td>
</tr>
<tr>
<td>High</td>
<td>Likely to occur once per month or less</td>
</tr>
<tr>
<td>Very High</td>
<td>Likely to occur multiple times per month</td>
</tr>
<tr>
<td>Extreme</td>
<td>Likely to occur multiple times per day</td>
</tr>
</tbody>
</table>

### Impact Severity Levels

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Little or no impact</td>
</tr>
<tr>
<td>Minor</td>
<td>Minimal effort to repair, restore or reconfigure</td>
</tr>
<tr>
<td>Significant</td>
<td>Small but tangible harm, noticeable to limited number, some effort to repair</td>
</tr>
<tr>
<td>Damaging</td>
<td>Damage or loss to a many, significant effort to repair</td>
</tr>
<tr>
<td>Serious</td>
<td>Considerable system outage, compromise of large amount information affecting many</td>
</tr>
<tr>
<td>Critical</td>
<td>Extended outage, permanent loss or damage, triggering business continuity procedures, complete compromise of information</td>
</tr>
</tbody>
</table>
This table shows the resulting risk level, for each degree of likelihood and each level of severity.

<table>
<thead>
<tr>
<th>Likelihood of Occurrence</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Significant</th>
<th>Damaging</th>
<th>Serious</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Very Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Very High</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Extreme</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
These tables document your analysis of the specific risks you might have to deal with.

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Threat Name</th>
<th>Vulnerability Name</th>
<th>Risk Description</th>
<th>Existing Controls</th>
<th>Likelihood of Occurrence</th>
<th>Impact Severity</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Flood</td>
<td>No off-site data back-up system</td>
<td>Loss of e- PHI</td>
<td>None</td>
<td>Very Low</td>
<td>Critical</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

2.

3.

4.
<table>
<thead>
<tr>
<th>Item No. (from Risk Determination Table)</th>
<th>Recommended Safeguard Description</th>
<th>Residual Likelihood of Occurrence</th>
<th>Residual Impact Severity</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Arrange for off-site data back-up</td>
<td>Very Low</td>
<td>Minor</td>
<td>Low</td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
C. Definitions of Key Terms

1. **Availability** means that data or information is accessible and usable on demand by an authorized person.

2. **Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.

3. **Integrity** means that data or information have not been altered or destroyed in an unauthorized manner.

4. **Risk** is defined in NIST SP 800-30 as “[t]he net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . [R]isks arise from legal liability or mission loss due to 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information; 2. Unintentional errors and omissions; 3. IT disruptions due to natural or man-made disasters; 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.”

    In brief: Risk is a function of (1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and (2) the resulting impact on the organization. So risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on your practice.

5. **Threat** is defined in NIST SP 800-30 as “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.” Threats may be natural, human, or environmental.

    Examples of common threats include: floods, earthquakes, tornadoes, and landslides (all natural); network and computer based attacks, malicious software upload, unauthorized access to e-PHI, inadvertent data entry or deletion and inaccurate data entry actions (all human); and power failures, pollution, chemicals, and liquid leakage (environmental).

6. **Vulnerability** is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

    Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access
to or disclosure of e-PHI. Vulnerabilities may be technical or nontechnical. Nontechnical vulnerabilities are, for example, ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities are such things as flaws or weaknesses in the development of information systems or incorrectly implemented or configured information systems.

D. Risk Analysis Summary

Risk analysis is the mandatory first step in your Security Rule compliance efforts. Risk analysis is an ongoing process that should result in a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.

The risk analysis is a careful and thoroughly documented evaluation of whether your practice’s administrative activities, physical environment, and computer systems are secure. The risk analysis will help you to determine and document any security threats or vulnerabilities (e.g., floods, computer viruses, or break-ins) in your practice by comparing your current activities with the administrative, physical, and technological requirements of the Security Rule. As part of the risk analysis process, you must assess the likelihood and impact of identified threats and vulnerabilities and determine any necessary preventive and corrective actions.

Each stage of the risk analysis must be documented, and the completed risk analysis document added to your HIPAA compliance records. You will also need to update relevant policy and procedure documents to reflect any administrative, physical, or technical safeguards that have been implemented as a result of the risk analysis. As you work through your risk analysis, you may notice that you have already complied with certain Security Rule standards in your efforts to comply with the Privacy Rule.

IV. SECURITY RULE STANDARDS AND IMPLEMENTATION SPECIFICATIONS

The Security Rule sets forth specific Standards that explain how to meet the Rule’s requirements.

A. The Standards are organized into three categories:

1. Standards for Administrative Safeguards that address the implementation of office policies and procedures, staff training, and other measures designed to carry out security requirements;

2. Standards for Physical Safeguards that relate to limiting access to the physical areas in which electronic information systems are housed; and

3. Standards for Technical Safeguards that concern authentication, transmission, and other issues that arise when authorized personnel access e-PHI via computer or other electronic device.
B. The Standards are designed to allow flexibility in compliance:

1. **No One-Size-Fits-All Compliance Program**

   The Security Rule is designed to permit some flexibility in compliance so that you can adopt the security measures that are best suited to your particular situation and needs - as long as you meet the Standards specified in the Security Rule. **There is no “one-size-fits-all” compliance program.** Rather, what you do to come into compliance will depend on the size, complexity, and capabilities of your practice. What works for a small practice may not work for a larger one.

2. **Scalability**

   The Security Rule’s “scalability” concept allows you to tailor your compliance process to the size, complexity, and capabilities of your practice. In determining how to comply with the Security Rule, consider the following factors as they relate to your practice:

   - size
   - complexity
   - capabilities
   - technical infrastructure
   - cost of procedure to comply
   - potential security risks

   For example, the Security Rule requires you to designate a HIPAA Security Officer. For a solo practitioner, it would be unduly expensive to hire someone just to fill this role, and doing so would not make sense in light of the relatively limited complexity of security issues. Accordingly, it would be appropriate for the solo practitioner simply to designate herself as the Security Officer.

C. **Overlap**

   There is some overlap among the Standards. You may notice that as you meet one Standard, you may very well also have satisfied another.

   For example, one of the Standards for Physical Safeguards requires physical protection against unauthorized access to a physician’s computer. This Physical Standard may overlap with the Administrative Standard requiring you to limit access to e-PHI to appropriate personnel and it may also overlap with the Technical Standard requiring you to develop procedures to verify the identity of persons who access e-PHI. If the physician’s computer is in a locked office and can only be accessed by authorized employees, you will have met the Physical Standard. If only appropriate personnel have keys to the door, complying with the Physical Standard by locking the office will also meet the Administrative
D. Implementation Specifications

Accompanying the Standards as part of the Security Rule are Implementation Specifications that provide specific details on how to implement the Standards. Implementation Specifications offer guidance in deciding which tasks should be undertaken to comply with each Standard.

Not every Standard has an Implementation Specification, but some Standards have several. Standards that do not have Implementation Specifications are not optional, and you must make reasonable efforts to comply.

Each practice is different; what constitutes compliance for one practice may or may not constitute compliance for another. There may be several different ways for you to implement any given Standard. For example, you must have a Security Officer. You can implement that requirement by contracting with an outside firm or person, or by hiring someone to perform only that function, or by appointing one of your current employees to perform that function in addition to his other responsibilities, or by appointing yourself - all depending on the circumstances.

1. “Required” vs. “Addressable” Implementation Specifications

Because HIPAA applies to a wide range of entities from solo practitioners to large health care systems, the law recognizes the need for flexibility in how each entity complies with the Standards. To allow for flexibility and customization, the Implementation Specifications are divided into those that are “required” and those that are “addressable.”

2. “Required.”

If a Standard includes “required” Implementation Specifications, you must implement the Implementation Specifications.

3. “Addressable.”

If a Standard includes an “addressable” Implementation Specification, you have some latitude in tailoring your implementation of that Standard to your individual practice or, in some instances, to dispense with the Implementation Specification altogether.

- You must assess whether the “addressable” Implementation Specification is a reasonable and appropriate safeguard in your
particular situation. Ask how likely it is to contribute to protecting your e-PHI. If it is “reasonable and appropriate,” then you must implement it. But if it is not reasonable and appropriate, you may choose either:

(a) to implement an equivalent reasonable and appropriate measure; or

(b) not to implement it, if non-implementation is reasonable.

For example, under the Security Awareness and Training Standard there is an addressable Implementation Specification that Security Reminders (i.e., bulletins, e-mails) should be sent to staff about potential security threats. If you don’t have any staff, it would make no sense to implement this Implementation Specification.

- Whatever choice you make when dealing with an “addressable” Implementation Specification, you must document not only that choice but also the rationale, based on risk analysis, for your choice.

V. THE STANDARDS AND IMPLEMENTATION SPECIFICATIONS

A. Administrative Safeguard Standards and Implementation Specifications

Administrative Safeguard Standards require you to develop and implement policies and procedures to prevent, detect, contain, and correct security violations.

Those Standards (1 through 9), and their 21 Implementation Specifications (listed immediately following the Standard to which they apply (a, b, c, etc.) are:

1. “Assigned Security Responsibility.” Appoint a HIPAA Security Officer who will be responsible for developing and implementing security policies and procedures for your practice. There is no separate Implementation Specification; this is absolutely required.

2. “Security Management Process.” The Security Officer must create and implement policies and procedures that are designed to prevent, detect, contain, and correct HIPAA security violations.

   a. Risk analysis (required) (See detailed discussion above.)

   b. Risk management (required): Implement security measures to reduce risks and vulnerabilities.

   c. Sanction policy (required): Develop and apply sanctions against workforce members who don’t comply with security policies and procedures. You must implement a sanction policy that clearly
delineates consequences for violations of security policies and procedures by employees, agents, and contractors. Consequences could include re-training the employee who violated the policies and procedures, issuing a warning, or perhaps terminating the individual if the violation is egregious or if there are repeat offenses. Sanctions must be applied equally to all individuals, and the policy should apply to any and all violations. If you are in compliance with the Privacy Rule, you will already have a Privacy Rule sanction policy which could be modified to address both Privacy and Security Rule requirements.

d. **Information system activity review (required):** Implement procedures to review regularly all records of information system activity, such as audit logs, access reports, and security incident tracking reports.

3. **“Workforce Security.”** Implement policies and procedures to ensure that all employees have appropriate access to e-PHI. Also ensure that those employees who should not have access are unable to access e-PHI.

a. **Authorization and supervision (addressable):** Implement procedures for the authorization and supervision of employees who work with e-PHI or who work in areas where e-PHI might be accessed.

b. **Workforce clearance procedure (addressable):** Implement procedures to determine that employee access to e-PHI is appropriate. The goal is to ensure that individuals who have access to e-PHI have appropriate clearance, such as a background check for employees who deal with e-PHI. Because this Specification is addressable, you can assess what is reasonable in your circumstances. For example, if you are the only employee, you would not need to undertake a clearance procedure on yourself. But remember that you must still document why the Specification does not apply (e.g., the only employee is yourself). In a small community and a practice with only a few employees who all come from that community, a reasonable effort to meet this Specification might be to call a prospective employee’s references and ask about her reliability and trustworthiness. In a larger organization, a formal background check (e.g., criminal record, bankruptcy, etc.) may be necessary to be considered compliant.

c. **Termination procedures (addressable):** Implement procedures for terminating access to e-PHI when employment ends.
4. “Information Access Management.” Implement policies and procedures on how your employees will be given access to e-PHI and how access will be limited when appropriate.
   
a. Isolate health care clearing house functions (required).
   
b. Access authorization (addressable): Implement policies and procedures for granting access to e-PHI, e.g., through access to a workstation.
   
c. Access establishment and modification (addressable): Implement policies and procedures to establish, document, review, and modify a user’s right of access to workstations, programs, transactions, etc.
   
5. “Security Awareness and Training.” Implement a security awareness and training program for all members of your workforce.
   
a. Security reminders (addressable): periodic security updates
   
b. Protection from malicious software (addressable)
   
   
d. Password management (addressable): Implement procedures for creating, changing, and protecting passwords.
   
6. “Security Incident Procedures.” Implement policies and procedures to address breaches of security.
   
a. Response and reporting (required): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security breaches; document security incidents and their outcomes.
   
7. “Contingency Plan.” Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrences that threaten the security of e-PHI, such as fire, vandalism, system failure, natural disaster, or theft.
   
a. Data backup plan (required): Implement procedures to create and maintain exact copies of e-PHI.
   
b. Disaster recovery plan (required): Establish procedures to restore any loss of data.
c. Emergency mode operation plan (required): Establish plan for continuation of critical business and security of e-PHI while operating in emergency mode.

d. Testing and revision procedures (addressable): Implement procedures for periodic testing and revision of contingency plans.

e. Applications and data criticality analysis (addressable): Assess relative criticality of specific applications and data in support of other contingency plan components.

8. “Evaluation.” Regularly evaluate all technical and nontechnical systems to ensure that e-PHI is adequately protected, especially if you have recently updated your risk analysis. You must also evaluate all technical and nontechnical systems in response to any environmental or operational changes affecting the security of e-PHI. Evaluations should be documented and should explain how your policies and procedures comply with the Security Rule requirements. There is no separate Implementation Specification; this is required.

9. “Business Associate Contracts.” Initiate policies and procedures to ensure that all business associate contracts between you and your business associates incorporate and pass along to the business associate the same obligations that you have as a covered entity to comply with the Security Rule.

a. Written contract or other arrangement (required): this contract or agreement can be combined with an existing Privacy Rule BA contract.

B. Physical Safeguard Standards

Physical Standards require implementation of policies and procedures that limit physical access to electronic information systems (e.g., computers) and the facilities (e.g., an office) in which e-PHI is housed. The physical “procedure” might be as simple as a lock on the door of the room in which the computers are located or as complex as a retinal scan, depending what is reasonable in any given circumstance.

The Physical Safeguard Standards and their 8 Implementations Specifications are:

1. “Facility Access Controls.” Implement policies and procedures to limit physical access to e-PHI systems and the facilities in which they are housed, while ensuring the properly authorized access is allowed.

2. Contingency operations (addressable): Establish procedures to allow facility access to support restoration of lost data under the disaster recovery plan and emergency mode operation. For example, create a
process to allow certain individuals to retrieve backup data and transfer that data to a different computer system in emergency circumstances, such as a hurricane or electrical storm. If you have dealt with this security concern through compliance with another Implementation Specification (e.g., a technical measure that automatically backs up critical e-PHI to a remote computer) or if your risk analysis has determined that this is not a significant risk, then you may not need to implement this Specification. It will not, however, be sufficient documentation just to state “not a risk.” Your explanatory documentation must provide details showing why it is not a risk.

3. **Facility security plan (addressable):** Implement policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering, and theft.

4. **Access control and validation procedures (addressable):** Implement procedures to control and validate a person’s access to facilities based on his role or function, including visitor control, and control of access to software for testing and revision.

5. **Maintenance records (addressable):** Implement policies and procedures to document repairs and modifications to the physical parts of the facility related to security, e.g., hardware, screens, walls, doors, locks.

6. **“Workstation Use.”** Implement policies and procedures that describe appropriate functions for a specific workstation (for example, a cubicle) or class of workstations used to access e-PHI. For example, restrict the e-PHI available on a reception area computer to only the e-PHI needed to schedule or change appointments. There is no separate Implementation Specification for this Standard; it is required.

7. **“Workstation Security.”** Physical mechanisms must be in place to ensure that access to workstations with e-PHI is restricted to authorized users. For example, have computer screens turned so they cannot be seen by casual observers. There is no separate Implementation Specification for this Standard; it is required.

8. **“Device and Media Controls.”** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain e-PHI into, within, and out of your facility.

   a. **Disposal (required):** Implement policies and procedures that take care of the final disposition of e-PHI and the hardware or electronic media on which it is stored.

   b. **Media re-use (required):** Implement policies and procedures for removal of e-PHI from media before they are re-used.
c. **Accountability (addressable):** Keep a record of the movements of hardware and electronic media and any person who is responsible for those movements.

d. **Data backup and storage (addressable):** Create a retrievable, exact copy of e-PHI as necessary before moving equipment.

### C. Technical Safeguard Standards

Technical Standards require you to have in place policies and procedures that govern the technical aspects of accessing e-PHI within computer systems, such as, computer passwords and encryption software.

The Technical Safeguard Standards and their Implementation Specifications are:

1. **“Access Controls.”** Implement policies and technical procedures for computer use to ensure only appropriate access to e-PHI by authorized individuals and software programs.

   a. **Unique user identification (required):** Assign a unique name or number for identifying and tracking user identity; sharing user identifications is not permitted.

   b. **Emergency access procedure (required):** Establish procedures of obtaining e-PHI in an emergency.

   c. **Automatic logoff (addressable):** Implement electronic procedures that terminate a session after a pre-determined period of inactivity.

   d. **Encryption and decryption (addressable):** Implement a mechanism to encrypt and decrypt e-PHI.

2. **“Audit Controls.”** Implement hardware, software, and procedural mechanisms that record and monitor activity on systems containing e-PHI for security breaches. For example, create a log that shows who accessed a particular computer and when. There is no separate Implementation Specification for this Standard; it is required.

3. **“Integrity.”** Implement policies and procedures to protect e-PHI from improper alteration or destruction.

   a. **Mechanism to authenticate e-PHI (addressable):** Create mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized way.

4. **“Person or Entity Authentication.”** Implement procedures to verify that a person or entity seeking access to e-PHI is in fact who he/it claims to be.
There is no separate Implementation Specification for this Standard; it is required.

5. **“Transmission Security.”** Implement technical security measures to guard against access to e-PHI that is being transmitted over an electronic communications network. For example, use secure transmission systems or encryption when e-mailing or transmitting patient data.

   a. **Integrity controls (addressable):** Implement measures to ensure that e-PHI is not improperly modified without detection.

   b. **Encryption (addressable):** Implement a mechanism to encrypt e-PHI as appropriate. In a larger practice with established policies and procedures for sharing encryption “keys” with authorized entities, purchasing a computer program that encrypts and decrypts data may be an appropriate way to handle this requirement. A small practice may choose to use a HIPAA-compliant secure messaging service that meets the security goal without encryption software.

**VI. COMPLIANCE DOCUMENTATION**

For all Security Rule Standards and Implementation Specifications, you must keep a written policies and procedures document (it may be in electronic format) that explains how you have complied with each step of implementation.

This document must be kept for 6 years from either the date it was created or the date it last went into effect, whichever is later, and the document must be made available to those persons responsible for implementing the procedures.

You must promptly update your policies and procedures to comply with any changes in the law or any changes in how you plan to comply with the Standards.
VII. GOVERNMENT ENFORCEMENT AND PENALTIES

The Security Rule is enforced by the Center for Medicaid and Medicare Sciences (CMS). HITECH now also permits enforcement by the Attorney General of each State. Failure to comply with the Security Rule may result in the following enforcement actions or civil or criminal penalties:

- CMS administratively imposes a corrective action plan
- civil Penalties ranging from $100 to $25,000 for each violation
- fines of up to $250,000 and imprisonment for up to 10 years

(These same penalties can be imposed for Privacy Rule violations; however, the Privacy Rule is enforced by the Office of Civil Rights (OCR).)