Norris McLaughlin & Marcus, P.A.
ATTORNEYS AT LAW

HIPAA SECURITY FOR THE PHYSICIAN PRACTICE

DISCLAIMER

This document is provided solely for informational purposes and to assist the typical physician practice which must undertake reasonable measures to comply with HIPAA Rules. While the document has been drafted to provide accurate and authoritative assistance, it is not intended as, and does not constitute legal or other professional advice, which can be rendered only on an individual practice and fact-sensitive basis. The information in it is not guaranteed to be correct, complete or up-to-date. Each practice must review this document for individualized adaptation to your practice or to a particular transaction. Readers should not act or elect not to act based upon the provided information without seeking professional legal advice from healthcare counsel.

HIPAA SECURITY FOR THE PHYSICIAN PRACTICE

Table of Contents

HIPAA Security for the Physician Practice

Introduction

The HIPAA Security Rule is part of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), passed by Congress to, among other things, protect the privacy and security of certain health information, and promote efficiency in the health care industry through the use of standardized electronic transactions. The Department of Health and Human Services (HHS) has published rules implementing many of the HIPAA provisions, including:

- Privacy Rule
- Electronic Transactions & Code Sets Rule
- National Identifier requirements for employers, providers, and health plans
- Security Rule (the final Security Rule can be obtained through links in the Tools section)

Who Must Comply?

All entities covered under HIPAA must comply with the Security Rule, including:

- Covered Health Care Providers – Any physician or provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard
- Health Plans – Any individual or group plan that provides or pays the cost of health care, such as a health insurance issuer and the Medicare and Medicaid programs
- Health Care Clearinghouses – A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa

If a Practice is required to comply with the Privacy Rule or the Electronic Transactions and Code Sets Rule of HIPAA, then it must comply with the Security Rule, as well. For more information on who is a covered entity under HIPAA, visit the Office for Civil Rights (OCR) website at http://www.hhs.gov/ocr/hipaa.

What Information is Affected?

The Security Rule applies to protected health information (PHI) that is in electronic form (EPHI). This includes EPHI that is created, received, maintained or transmitted. For example, EPHI may be transmitted over the Internet or stored on a computer, CD, disk, magnetic tape, or other related means.

Practice Pointer: "Electronic Media" is defined in the Security Rule as: (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet or intranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission.

Unlike the Privacy Rule, which applies to all forms of PHI, whether electronic, written or oral, the Security Rule does not apply to PHI that is transmitted or stored on paper or provided orally. It does not apply to paper-to-paper faxes or video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission.

The Privacy Rule already requires covered entities to have in place appropriate administrative, physical, and technical safeguards and to implement those safeguards reasonably--a sort of "mini Security Rule." In effect, a Practice that has implemented those safeguards may find that it has already taken some of the measures necessary to comply with the Security Rule. Specifically, 45 CFR § 164.530(c) of the Privacy Rule contains the following provisions:

(c)(1) <u>Standard: safeguards.</u> A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) <u>Implementation specification: safeguards.</u> A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

The Security Rule requires more detailed and comprehensive security requirements. However, a Practice should assess what security initiatives they have already implemented to comply with the Privacy Rule.

Note: As with the Privacy Rule, state laws that are contrary to the Security Rule are preempted by the Federal requirements, unless a specific exception applies.

HIPAA Security for the Physician Practice

Deadlines and Enforcement

Compliance Deadline

Compliance with the Security Rule was required effective April 20, 2005, except for small health plans which had to comply by April 20, 2006.

Enforcement

The Office for Civil Rights (OCR) within HHS oversees and enforces the Security Rule and the Privacy Rule. There are both civil and criminal penalties for non-compliance with the Security Rule's requirements. OCR has adopted an enforcement rule which can be found at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html/

Note: Non-compliance with the HIPAA Privacy and Security Rules could create liability under state law. HIPAA standards potentially create a standard of care that could support a state law claim.

HIPAA Security for the Physician Practice

Provisions of the Security Rule

General Requirements of the Security Rule

The Security Rule requires a covered entity to implement measures that are intended to:

- Ensure the confidentiality, integrity, and availability of all of its EPHI
- Protect against reasonably anticipated threats or hazards to the security of such information
- Protect against reasonably anticipated uses or disclosures of EPHI that are not permitted or required by the Security Rule
- Ensure compliance with the Security Rule by its workforce

Confidentiality means that EPHI is accessible only by authorized people and processes.

Integrity means that EPHI is not altered or destroyed in an unauthorized manner.

Availability means that EPHI can be accessed as needed by an authorized person.

Standards and Implementation Specifications

The specific requirements of the Security Rule are found at 45 CFR Part 164, Subpart C within the following subparts:

164.302 - Applicability
164.304 - Definitions
164.306 - Security standards: General rules
164.308 - Administrative safeguards
164.310 - Physical safeguards
164.312 - Technical safeguards
164.314 - Organizational requirements
164.316 - Policies and procedures & documentation requirements
164.318 - Compliance dates for the initial implementation of the security standards

In complying with the Security Rule, it is important to understand how each requirement must be addressed. The requirements are broken down into "standards" and "implementation specifications" ("specs," if you will). A "standard" is a general requirement that must be met by a covered entity. An "implementation specification" is an additional detailed instruction for implementing a particular standard.

Required versus Addressable

Each set of safeguards (for example, administrative, physical, and technical safeguards) is comprised of a number of standards which, in turn, are comprised of a number of implementation specifications. Each implementation specification is either "required" or "addressable." **Note:** A concise matrix of the standards and implementation specifications, and whether the specifications are "required" or "addressable," is set forth in the Security Rule which can be accessed via websites = listed in the Tools section of this guidebook.

If an implementation specification is "required," the Practice must implement policies and/or procedures that meet what the implementation specification requires. If an implementation specification is "addressable," then the Practice must assess whether it is a reasonable and appropriate safeguard in the Practice's environment. This means analyzing the specification in reference to the likelihood of protecting the Practice's EPHI from reasonably anticipated threats and hazards.

"Addressable" does not mean the Practice need do nothing. If the Practice chooses not to implement an addressable specification based on its assessment, it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure. For each of the addressable implementation specifications, a Practice must do one of the following:

- Implement the specification if reasonable and appropriate; or
- If implementing the specification is not reasonable and appropriate
    - Document the rationale supporting the decision and
    - Implement an equivalent measure that is reasonable and appropriate and that would accomplish the same purpose or
    - Not implement the addressable implementation specification or an equivalent alternative measure, if the standard could still be met and implementing the specification or an alternative would not be reasonable or appropriate

If a given addressable implementation specification is determined to be reasonable and appropriate, the Practice must consider options for implementing it. The decision regarding what security measures to implement to address the standards and implementation specifications will depend on a variety of factors, including:

- The Practice's risk analysis – What current circumstances leave the Practice open to unauthorized access and disclosure of EPHI?
- The Practice's security analysis – What security measures are already in place or could reasonably be put into place?
- The Practice's financial analysis – How much will implementation cost?

Depending on the complexity of a Practice, it may have and require less technology, have a lower risk of inappropriate use and disclosure of EPHI, and have fewer funds to spend on security measures.

Flexible and Scalable Standards

The requirements of the Security Rule were designed to be technology neutral, meaning the security standards do not dictate or specify the use of specific technologies. The security standards are also scalable from the very largest health plan to the smallest physician practice. Compliance with the Security Rule will require an evaluation of what security measures are currently in place, an accurate and thorough risk analysis, and a series of documented solutions derived from a number of complex factors unique to each entity.

HHS acknowledges that there is no such thing as a totally secure system. The Security Rule was designed to provide guidelines to all types of covered entities, affording flexibility in how to implement the security standards. Covered entities may use appropriate security measures that enable them to reasonably implement a standard. In deciding which security measures to use, a covered entity should take into account its size, capabilities, the cost of the specific security measures, and the operational impact.

Practices will be expected to balance the risks of inappropriate use or disclosure of EPHI against the impact of various protective measures. This means that smaller and less sophisticated practices may not be able to implement security in the same manner, and at the same cost, as larger and more complex practices. However, **cost alone is not an acceptable reason to not implement a procedure or measure**. Specifically, 45 CFR § 164.306(b) requires that the following factors be considered when determining how to implement a standard:

- The size, complexity, and capabilities of the covered entity
- The covered entity's technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to EPHI

The Practice must periodically evaluate, and modify as necessary, its security measures to try to ensure that such measures continue to provide reasonable and appropriate protection of the Practice's EPHI.

HIPAA Security for the Physician Practice

Administrative Safeguards

What are they?

Administrative safeguards (45 CFR § 164.308) are the administrative functions that should be implemented to meet the requirements of the Security Rule. They focus on the Practice's workforce and the policies and procedures necessary to implement such things as responsibility, training, and a contingency plan. Specifically, the administrative safeguards include the following standards (each standard and its implementation specifications are detailed below):

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts & Other Arrangements

Standard: Security Management Process – Implement policies and procedures to prevent, detect, contain, and correct security violations.

Implementation Specifications:

- **Risk Analysis (Required)** – Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI (see definition of these terms under Provisions of the Security Rule) held by the Practice

- **Risk Management (Required)** – Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

- **Sanction Policy (Required)** – Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Practice

- **Information System Activity Review (Required)** – Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

Practice Pointers: This standard requires that you assess, implement, enforce and review your security measures. The process begins with risk analysis to determine what vulnerabilities exist to the security of the Practice's EPHI. Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the EPHI held by the Practice, and the likelihood of occurrence. See the Tools section of this guidebook for further OCR Guidance on Risk Analysis.

A system vulnerability is a flaw or weakness in a system, due to its design, installation, lack of policies and procedures, or some other cause. Any of these weaknesses, whether intentional or accidental, could potentially result in a breach or inappropriate use or disclosure of EPHI. Examples of such vulnerabilities are those caused by ineffective policies regarding user names and passwords, holes or weaknesses in some of the software tools, or flaws in the operating system or application, or inadequate access controls.

The risk analysis may include inventorying of all systems and applications that are used to store, access, process, receive and transmit data, and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss of or damage to data, corrupted data systems, and anticipated ramifications of such losses or damage. Next is a review of all existing policies and procedures the Practice has in place that affect security and privacy of PHI. This includes a review of office manuals, personnel manuals, and standard operating procedures. This review may reveal that the Practice already has in place adequate protection of EPHI. More likely, the risk analysis will reveal that there are certain security risks that have not been addressed by the Practice, at least not in the way required by the Security Rule and documented. The risk analysis will allow the Practice to determine what level of risk the Practice can accept and how to reduce security risks to that reasonable level.

As discussed under Provisions of the Security Rule, determining what measures the Practice should take requires weighing the following factors:

- *The size, complexity, and capabilities of the covered entity*
- *The covered entity's technical infrastructure, hardware, and software security capabilities*
- *The costs of security measures (NOT the only factor to consider)*
- *The probability and criticality of potential risks to EPHI*

Risk management is the actual implementation of security measures to sufficiently reduce a Practice's risk of losing or compromising its EPHI and to meet the general security standards. It is not a static process to be undertaken only at the beginning of security compliance. Risk management requires periodic review of the processes put into place and updating those processes to address new or changed risks.

Implementing a security sanctions policy may simply mean updating the Practice's existing sanctions policy implemented under the Privacy Rule. That policy should clearly advise owners, employees, and agents of what the Practice's policies are and what disciplinary steps will be taken to address violations.

An Information System Activity Review is a long way of saying "auditing." Fortunately, many computer programs have automatic audit functions that can be used to monitor system activity. Alternatively, software can be purchased that will perform the same function. Small practices may be able to rely on physical and technical safeguards (discussed under Physical Safeguards and Technical Safeguards) to control access to EPHI and, thus, may not require the technology appropriate to the larger practice. In any case, however, the Practice must document why it chose a particular auditing mechanism.

Standard: Assigned Security Responsibility – Identify the person in the Practice who will serve as the security officer who is responsible for developing and implementing the policies and procedures required by the Security Rule.

Practice Pointers: As with the Privacy Rule, a Practice must designate a person as the security "official" who is responsible for both developing and implementing the Practice's security policies and procedures. This may be one and the same person, or may be a different person than the Privacy Officer and it may be filled by an administrative staff person or by a physician. Although ultimate responsibility rests with one person, more than one individual may be given specific security responsibilities within the Practice. The Practice must document the assignment of these responsibilities.

Standard: Workforce Security – Implement policies and procedures to ensure that all members of the Practice's workforce have appropriate access to EPHI, and to prevent those workforce members who do not have access from obtaining access to EPHI.

Implementation Specifications:

- **Authorization and/or Supervision (Addressable)** – Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed

- **Workforce Clearance Procedure (Addressable)** – Implement procedures to determine that the access of a workforce member to EPHI is appropriate

- **Termination Procedures (Addressable)** – Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made pursuant to the Practice's workforce clearance procedure

Practice Pointers: This standard requires determining who in the Practice should have authority to access what EPHI. For small practices, this may mean every person has authority to access all EPHI. Larger practices may use a role-based analysis to determine who should have access to EPHI. The policy on authorization may be an extension of the Practice's "minimum necessary" requirements in the Practice's existing Privacy policy on access. The policy should be revised to include who has access to which computer systems, as well as providing for the supervision of maintenance personnel and vendors who come to the Practice.

The employee's job description can state the authority and level of access granted to the staff person. Even if the Practice, because of its size, does not implement a policy and procedure regarding authorization and supervision, it must document the reasons for that decision.

Workforce clearance should already be a part of the Practice's standard operating procedures. This falls under the Practice's hiring procedures, as well as determining who is cleared to have a key to the office or to particular locations that house PHI.

Just as clearance at the beginning of an employee's tenure with the Practice establishes the employee's authorization and access to EPHI, the termination of that employee must involve a "de-authorization" process. The Practice should require that all employees and independent contractors who leave the Practice return keys or other tools they were given to access the building, the office premises, or equipment. The Practice should also change locks, remove the person's name and password from user accounts, and test that the person's access has, in fact, been disabled. The security officer should document that these procedures were followed in each instance.

Standard: Information Access Management – Implement policies and procedures for authorizing access to EPHI.

Implementation Specifications:

- **Isolating Health Care Clearinghouse Functions (Required)** – If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization. **Note**: Although this implementation specification is not applicable to physician practices, because it is a required specification practices must simply document that it is not applicable to them

- **Access Authorization (Addressable)** – Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process or other mechanism

- **Access Establishment and Modification (Addressable)** – Implement policies and procedures that, based upon the Practice's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program or process

Practice Pointers: This standard requires implementation and documentation, through a written policy and procedure, granting access to EPHI to those persons who have been authorized under this standard. The policy should be as detailed as is necessary based on the size of the Practice and the complexity of the levels of access it grants to its personnel. The access control standards, under Technical Safeguards, require policies procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

Standard: Security Awareness and Training – Implement a security awareness and training program for all members of the Practice's workforce, including management.

Implementation Specifications:

- **Security Reminders (Addressable)** – Periodic security updates
- **Protection from Malicious Software (Addressable)** – Procedures for guarding against, detecting, and reporting malicious software
- **Log-in Monitoring (Addressable)** – Procedures for monitoring log-in attempts and reporting discrepancies
- **Password Management (Addressable)** – Procedures for creating, changing, and safeguarding passwords

Practice Pointers: The first step in complying with this standard is to take note of the requirement that "all" members of the Practice's workforce are affected, including physicians and management. A security awareness and training program means training the workforce on the vulnerabilities of the Practice's EPHI and the policies and procedures in place to protect that information. Training should include information about how security incidents or problems should be reported. All training activities should be documented.

Training need not include third parties who access the Practice's EPHI, such as vendors, but the obligation of these parties to protect the Practice's PHI should be addressed in a Business Associate Agreement.

After initial training is completed, reminders should be provided to staff using the methods typically utilized by the Practice to keep staff informed, such as staff meetings and notices. Security updates should be utilized, especially if the Practice's operations change, such as beginning Internet use, implementing a new computer application, etc.

To protect the Practice's computer systems from malicious software, the Practice should have virus protection software which also provides for automatic reporting when viruses are detected. Such software—and upgrades--should be properly installed. Personnel should be prohibited from opening any e-mails or attachments from an unknown source, especially executable files or software programs (files that end with ".exe"). The Practice should prohibit staff from personal Internet use at the office and from downloading software, games, etc.--policies which may already be included in your personnel manual and simply require updating for the Security Rule. Computers should be checked periodically for compliance with this policy. Staff should be made aware through a written policy that the employee should have no personal expectation of privacy when it comes to information that the employee transmits, receives or stores on the Practice's computers.

The Practice should confirm with its software vendor what other capabilities the Practice's software has to protect the Practice's EPHI. For example, the Practice's software should limit

the number of log-in attempts to access EPHI. The software should have a function that notifies the Security Officer if the maximum number of attempts is exceeded and lock out the user.

The use of passwords is common to nearly every Practice and clear policies must be in place to prohibit posting, sharing and disclosing passwords. A policy should be in place as to how passwords will be created in order to have passwords that are less likely to be ascertainable by unauthorized persons. In addition to desktop computers, all laptops, mobile devices, and similar devices used by physicians or others in the Practice to store or transmit EPHI must be password protected.

Standard: Security Incident Procedures – Implement policies and procedures to address security incidents.

Implementation Specifications:

- **Response and Reporting (Required)** – Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Practice; and document security incidents and their outcomes.

Practice Pointer: The Security Rule defines a security incident as "an attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system." Examples are having a computer infected with a virus, a staff member sharing a password in violation of Practice policy, and unauthorized persons accessing EPHI. The Practice's policies and procedures, including the Practice's Data Breach Notification Policy, should include how and to whom security incidents are reported and how the incident will be addressed.

Standard: Contingency Plan – Establish (and implement, as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure or natural disaster) that damages systems that contain EPHI.

Implementation Specifications:

- **Data Backup Plan (Required)** – Establish and implement procedures to create and maintain retrievable exact copies of EPHI

- **Disaster Recovery Plan (Required)** – Establish (and implement, as needed) procedures to restore any loss of data

- **Emergency Mode Operation Plan (Required)** – Establish (and implement, as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode

- **Testing and Revision Procedure (Addressable)**- Implement procedures for periodic testing and revision of contingency plans

- **Applications and Data Criticality Analysis (Addressable)** – Assess the relative criticality of specific applications and data in support of other contingency plan components

Practice Pointer: Disasters can strike a Practice of any size and despite taking all reasonable precautions to prevent them. Fires, floods, equipment failures, power outages, and vandalism are all possible scenarios. Every Practice must have a contingency plan that includes, at the minimum, a data backup plan and a disaster recovery plan. Practices must have a method for copying the Practice's data to another medium from which lost data can be recovered. Computer software can provide an automatic backup process and the backup tapes should be stored off-site and off-network in a secure location. In determining what backup plan is needed, assess how critical the information is to the Practice (can you survive one day without electronic records or a working network or only 15 minutes? How quickly will patient health be affected?). Test your backup plan before you need it.

If a disaster occurs that prevents access to the Practice's computers, there should be a pre-determined and secure computer on which to run the back-up. The Security Officer should have procedures in place for appropriate notifications to employees, patients, vendors, and business associates if the Practice's operations have been interrupted, and procedures for what will be done to get the Practice up and running as quickly as possible. Part of these procedures is determining which computer applications are the most critical and should be the first to be restored.

Standard: Evaluation – Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which a Practice's security policies and procedures meet the requirements of the Security Rule.

Practice Pointer: Compliance with these standards is not a one-time goal but must be maintained over time through evaluation to verify secure EPHI transmission, storage, backup, and access. Subsequent evaluations—at least an annual internal audit-- will allow the Practice to address how well the Practice has implemented its security measures and whether it has addressed environmental or operational changes that affect the security of the Practice's EPHI. Documenting the evaluation required by this standard will help prove that the Practice made all reasonable efforts to secure its EPHI.

Note: *There is no standard or implementation specification that requires a Practice to "certify" compliance with the Security Rule or to retain any outside organization to provide evaluation or certification services to the Practice. The evaluation standard requires the Practice to perform a periodic evaluation that establishes the extent to which the Practice's policies and procedures meet the security requirements.*

Standard: Business Associate Contracts and Other Arrangements – A Practice may permit a business associate to create, receive, maintain or transmit EPHI on the Practice's behalf only if the Practice obtains satisfactory assurances that the associate will appropriately safeguard the information.

Implementation Specifications:

- **Written Contract or Other Arrangement (Required)** – Document the satisfactory assurances required by this standard through a written contract or other arrangement with the business associate

Practice Pointer: Under the Privacy Rule, all covered entities already should have in place a Business Associate Agreement with third parties that perform services for the Practice which allow the third party to gain access to the Practice's PHI. If any of those business associates uses or accesses the Practice's EPHI, that Business Associate Agreement must be updated to incorporate compliance with the Security Rule. All Business Associate Agreements should also incorporate the Business Associate's Data Breach Notification obligations.

Note: This standard does not apply with respect to certain transmissions of EPHI, including the transmission of EPHI by a covered entity to a health care provider concerning the treatment of an individual, unless the covered entity is providing services on behalf of the provider that create a business associate relationship.

HIPAA Security for the Physician Practice

Physical Safeguards

What are they?

Physical safeguards (45 CFR § 164.310) are the mechanisms required to protect electronic systems, equipment, and the data they hold, from threats, environmental hazards and unauthorized intrusion. They are physical measures, policies, and procedures to protect a Practice's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. They focus on the Practice's physical actions and set-up designed to ensure that only authorized persons have physical access to the Practice's facilities, equipment, and EPHI. Specifically, the physical safeguards include the following standards (each standard and its implementation specifications are detailed below):

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and media controls

As with many aspects of the Security Rule, different practices will have different issues and challenges in complying with the Physical Safeguards Standards, depending upon such things as the size of the Practice's workforce and whether the Practice's physical facility is freestanding or part of a building housing other businesses, and whether the office facility is owned and operated by the Practice. **Note:** Some aspects of the Physical Safeguards requirements are addressed under Administrative Safeguards.

Standard: Facility Access Controls – Implement policies and procedures to limit physical access to the Practice's electronic information systems and the facility or facilities in which it is housed, while ensuring that properly authorized access is allowed.

Implementation Specifications:

- **Contingency Operations (Addressable)** – Establish (and implement, as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency

- **Facility Security Plan (Addressable)** – Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft

- **Access Control and Validation Procedures (Addressable)** – Implement procedures to control and validate a person's access to facilities based on their

role or function, including visitor control, and control of access to software programs for testing and revision

- **Maintenance Records (Addressable)** – Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware walls, doors, and locks)

Practice Pointer: Securing the Practice's physical facility already should be part of the Practice's standard operating procedures. However, with security, the goal is to limit physical access to the facility and to the computer systems, while allowing properly authorized access. These needs may change with the circumstances, such as when the Practice's disaster recovery plan and emergency mode operations plan (discussed in Administrative Safeguards) are initiated, or when the Practice expands its operations or systems. The Security Rule requires a Practice to implement physical safeguards for its electronic information systems whether such systems are housed on the Practice's premises or at another location.

The minimum level of facility security for the Practice means taking reasonable steps to keep the facility properly locked after hours, with appropriate alarm systems to detect intruders, and preventing inappropriate access to EPHI during office hours. During hours of operation, the Practice should ensure that all entryways are visible for monitoring and that all areas where PHI could be accessed are suitably protected from unauthorized entry. The extent that the Practice's own workforce is limited in its access to different locations within the facility depends on the size of the workforce, the size of the facility, and the complexity of operations. The smaller the Practice, the more likely all members of the workforce will have access to all areas of the facility and all locations of PHI. Access by patients, those who accompany patients, vendors, reps, and others not members of the workforce, must be strictly limited.

Whenever the Practice makes repairs, upgrades or takes other steps to strengthen the security of its facility and systems, such activities should be documented as evidence of compliance with this standard.

Standard: Workstation Use – Implement 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 EPHI.

Standard: Workstation Security – Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users.

Practice Pointer: For nearly all practices, workstations present a security issue. The most basic of workstation use and security requirements already should have been addressed in the Practice's privacy policies and procedures (see Introduction and the "mini-security rule" from the Privacy Rule). This entails making sure that the computer itself cannot be accessed by unauthorized users and that the computer monitor is not viewable by "unauthorized eyes." If this cannot be accomplished by placing the computer and monitor in restricted areas, or by positioning computer monitors so that only authorized persons can view them, then privacy

screens, screensavers requiring password re-entry, and/or appropriate access controls (see above) must be implemented. Screensavers and passwords should be utilized for any device containing EPHI and staff should be trained on the proper procedures for logging on and off. Desktop computers are not the only "workstations" affected by the security rule. Laptops, cell phones, and mobile devices must also be use-restricted and secure. If one of these devices is taken from the Practice, there must be a sign in and sign out sheet.

Standard: Device and Media Controls – Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

Implementation Specifications:

- **Disposal (Required)** – Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored

- **Media Re-Use (Required)** – Implement procedures for removal of EPHI from electronic media before the media are made available for re-use

- **Accountability (Addressable)** – Maintain a record of the movements of hardware and electronic media and any person responsible therefore

- **Data Backup and Storage (Addressable)** – Create a retrievable, exact copy of EPHI, when needed, before movement of equipment

Practice Pointer: Part of the Practice's risk analysis (see Administrative Safeguards) should be taking an accurate inventory of all of the Practice's devices and electronic media, e.g., computers of all types, software, disks, CD's, etc. Then determine whether these devices and media are shared throughout the Practice and whether they always remain in the Practice facility or are sometimes removed from the facility. Policies and procedures should provide for logs that keep track of these items and for assigning responsibility for monitoring their movement both within the Practice facility, as well as when they are removed from the facility.

Many of the horror stories that have circulated about privacy and security breaches resulting in inappropriate disclosure of PHI resulted from the inadvertent sale or disposal of computers that were not first "cleaned" of all EPHI stored on their hardware. Some electronic devices and media, such as floppies and CD's, can be easily destroyed before disposal to make them unusable, while software programs may be needed to completely sanitize hardware on a computer. Similar software programs can clean media prior to its re-use.

The data backup and storage provisions of the Practice's Contingency Plan (see Administrative Safeguards) should include backing up data on any device that is to be moved, as moving the equipment could cause the loss of data.

HIPAA Security for the Physician Practice

Technical Safeguards

What are they?

Technical safeguards (45 CFR § 164.312) are primarily the automated processes used to protect data and control access to data. They focus on the Practice's efforts to implement controls that will authenticate and verify authority to access EPHI and to protecting data as it is being stored and/or transmitted. Specifically, the technical safeguards include the following standards (each standard and its implementation specifications are detailed below):

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Note: Some aspects of the Technical Safeguards requirements are addressed under Administrative Safeguards and/or Physical Safeguards.

Standard: Access Control – Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

Implementation Specifications:

- **Unique User Identification (Required) –** Assign a unique name and/or number for identifying and tracking user identity
- **Emergency Access Procedure (Required) –** Establish (and implement, as needed) procedures for obtaining necessary EPHI during an emergency
- **Automatic Logoff (Addressable) –** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
- **Encryption and Decryption (Addressable) –** Implement a mechanism to encrypt and decrypt EPHI

Practice Pointer: Access control is discussed throughout all of the safeguards, but the technical safeguard for access control can be met by most Practices by utilizing the features that are standard with computer operating and software packages. Every member of the Practice's workforce should have an assigned name and/or number for identifying the member who is accessing EPHI. Establishing unique user names and passwords—ones that cannot easily be detected—should have been implemented as a HIPAA privacy procedure and should be carried over and strengthened for HIPAA security.

Automatic logoffs that are triggered after a predetermined time of inactivity on the computer are an extension of the HIPAA privacy procedure of utilizing automatic screensavers (as a means of avoiding inappropriate "viewing" of computer screens). Each Practice in consultation with its technical support professional must determine, for each of its computers, the appropriate time period of inactivity that should trigger an automatic logoff.

Practices that allow employees to work at home or otherwise work remotely and have access to EPHI must implement appropriate safeguards to protect the Practice's data in those settings, such as through automatic logoffs on the employee's home computer. Because automatic logoff is an addressable implementation specification, a Practice that determines that this specification is not reasonable and appropriate for its security needs must document that decision and then implement an equivalent alternative measure or some other means for meeting the standard.

The Security Rule does not expressly prohibit the use of e-mail for sending EPHI. However, the standards for access control, integrity, and transmission security require a Practice to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to EPHI. Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code, or access to another confidential process, would be able to descript (translate) the text and convert it into plain, comprehensible text. Simply put, encryption means that information is coded or scrambled in a way that it cannot be read by anyone who does not have the "key" to decode and read it.

Practice Pointer: The use of encryption is an addressable implementation specification. Practices use open networks such as the Internet and e-mail systems differently, and no single inter-operable encryption solution for communicating over open networks exists. The Security Rule does not set a single encryption standard. However, under the federal Data Breach Notification Rule, covered entities and business associates need only provide notification of a breach that involved unsecured PHI, which is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology, e.g., encryption, or methodology specified by HHS in guidance, found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html and updated annually.

A Practice must assess its use of open networks, identify the available and appropriate means to protect EPHI as it is transmitted, select a solution, and document the decision.

Standard: Audit Controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

Practice Pointer: The activity on the Practice's electronic systems should be monitored to determine that no one has inappropriately gained access to the Practice's information systems or otherwise tampered with the Practice's EPHI. These audit controls could be in the form of reviewing logons and logoffs, file access, and invalid password attempts. Software can be configured to automatically audit such activities.

Standard: Integrity – Implement policies and procedures to protect EPHI from improper alteration or destruction.

Implementation Specifications:

- **Mechanism to Authenticate EPHI (Addressable)** – Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner

Practice Pointer: The vulnerability of the Practice's EPHI to alteration or destruction varies depending on how EPHI is used, stored, and transmitted by the Practice. If the Practice does not utilize the Internet, does not allow remote access or work from home, then the data is less at risk and implementing minimal access controls, such as passwords, may be sufficient mechanisms to ensure that data integrity is maintained.

However, if the Practice does have some of these vulnerabilities, it may be necessary to use virus protection, firewalls, and multiple access controls. Anti-virus software is discussed under Administrative Safeguards. Computer firewalls—designed to prevent unauthorized persons from logging onto the Practice's computer system via the Internet and sometimes regulating what is transmitted from *the system—are another relatively inexpensive technology for protecting a Practice's EPHI. First, determine if the Practice's computer system already has a firewall. Firewalls are built into some DSL and cable modems or the Practice's computer vendor may have installed a firewall. Some computer operating systems come with a firewall that must be turned on. Each Practice must investigate and assess how much protection it has and how much it needs.*

Standard: Person or Entity Authentication – Implement procedures to verify that a person or entity seeking to access EPHI is the one claimed.

Practice Pointer: Authentication has been discussed under Administrative Safeguards related to audit trails and password requirements. This standard reinforces the need for passwords and documentation of access to computer systems as a way to authenticate the person attempting to obtain access to EPHI. For example, whenever a staff member logs on to a computer using the designated user name and password, that person has been "authenticated."

Standard: Transmission Security – Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

Implementation Specifications:

- **Integrity Controls (Addressable)** – Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of

- **Encryption (Addressable)** – Implement a mechanism to encrypt EPHI whenever deemed appropriate

Practice Pointer: Transmission security means that the Practice's EPHI is protected during transmission and properly routed to the intended recipient. Many of the security measures that provide this protection are discussed above.

A Practice that has determined it is not necessary to implement encryption at the office, should be sure to consider other computer systems and devices used by the Practice that contain or process the Practice's EPHI and whether encryption is necessary to protect that data, such as use of a mobile device.

HIPAA Security for the Physician Practice

Organizational Requirements

What are they?

The Security Rule's organizational requirements (45 CFR § 164.314) are those requirements related to the Practice's relationship with its business associates. They focus on the Practice's written contract with its business associates and actions taken when a Practice is aware that a business associate is not complying with the contract. Specifically, the organizational requirements consist of one standard and its implementation specifications as detailed below.

Note: The HITECH Act made business associates subject to the Security Rule's administrative safeguards, physical safeguards, technical safeguards, and requirements related to policies, procedures, and documentation, related to EPHI. As of this date, final regulations have not been adopted to address all aspects of the contractual requirements between covered entities and their business associates.

Standard: Business Associate Contracts or Other Arrangements – The contract between the Practice and its business associates as required under the Security Rule (see Administrative Safeguards) must meet the implementation requirements set forth below. A covered entity is not in compliance with the HIPAA standards applicable to relationships with business associates if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach of violation of the business associate's obligation under the contract, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful: (1) terminated the contract or arrangement, if feasible; or (2) if termination is not feasible, reported the problem to the Secretary of HHS.

Implementation Specifications (Required):

- **Business Associate Contracts** – The contract between a Practice and a business associate must provide that the business associate will:
  - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains or transmits on behalf of the Practice, as required by the Security Rule
  - Ensure that any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it
  - Report to the Practice any security incident of which it becomes aware (which should be addressed as part of compliance with the Data Breach Notification Rule)

- **Other Arrangements** – An "other arrangement" option is available when the covered entity and its business associate are both governmental entities. If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit EPHI on its behalf to the extent necessary to comply with the legal mandate provided that the covered entity attempts in good faith to obtain satisfactory assurances as required, and documents the attempt and the reasons that these assurances cannot be obtained. The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

HIPAA Security for the Physician Practice

Policies & Procedures/Documentation Requirements

What are they?

The Policies and Procedures and Documentation requirements (45 CFR § 164.306) are the means by which a Practice formalizes and implements its decisions related to the Security Rule standards and implementation specifications. It is also how the Practice shows that it is complying with the Security Rule. Specifically, the Policies and Procedures and Documentation requirements include the following standards (each standard and its implementation specifications are detailed below):

- Policies and Procedures
- Documentation

Standard: Policies and Procedures – Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule (taking into account the flexibility and scalability of such compliance efforts, see Provisions of the Security Rule). A Practice may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Security Rule.

Practice Pointer: Policies and procedures to implement the Security Rule may vary, depending on the size and complexity of the Practice. The Security Officer is responsible for the development and implement of policies and procedures (although specific tasks may be delegated to other persons within the Practice).

The first step in determining what policies and procedures are needed to comply with the Security Rule is for the Practice to review all policies and procedures it already has in place. In addition to standard office procedures and personnel policies, practices that are covered entities under HIPAA already have policies and procedures in place to comply with the Privacy Rule, including the "mini-security rule" within the Privacy Rule (see Introduction). This "gap analysis" reveals what additional policies and procedures are needed or what modifications should be made to existing ones in order to implement the Security Rule's requirements. Workforce members should then be trained on the revised and expanded policies and procedures.

Standard: Documentation – Maintain the policies and procedures implemented to comply with the Security Rule in written form (which may be electronic). If an action, activity or assessment is required by the Security Rule to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.

Implementation Specifications:

- **Time Limit (Required)** – Retain the documentation required by this standard for 6 years from the date of its creation or the date when it last was in effect, whichever is later
- **Availability (Required)** – Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains
- **Updates (Required)** – Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI

Practice Pointer: Documentation should be detailed enough to communicate the security measures taken and to facilitate periodic evaluations. The Security Officer, or her or his designate, must be responsible for maintaining and updating the Practice's security policies and procedures, including developing a timeline to review and update existing policies. The need to review and update security measures will vary depending on a Practice's size, complexity, operational changes, and new security measures implemented.

As part of documentation, Practices should remember to document all decisions made regarding the Security Rule's standards and implementation specifications, including the reasoning behind a decision not to implement an addressable specification.

Note: The preamble of the Security Rule's documentation provision specifically states that a Practice is required to document various actions, activities, and assessments. A Documentation Checklist can be found in the Tools section of this guidebook.

HIPAA Security for the Physician Practice

Tools

Office for Civil Rights – Security Rule materials:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Guidance on Risk Analysis Requirements under the Security Rule
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

Privacy and Security Resources – Office of the National Coordinator for Health Information Technology)
http://www.healthit.gov/providers-professionals/ehr-privacy-security

The HIPAA Omnibus Rule can be found at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html

Required versus Addressable Implementation Specifications Matrix – attached hereto

Appendix A to Subpart C of Part 164 – Security Standards: Matrix

Administrative Safeguards

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

Physical Safeguards

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

Technical Safeguards

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