Introduction

Eagle Associates, Inc.

Eagle Associates provides compliance services for over 1,200 practices nationwide. Services provided by Eagle Associates address compliance for OSHA, HIPAA, OIG, and CLIA regulations and guidelines. Eagle Associates has been providing services since 1986.

Call 800-777-2337 for information on services

Joseph Suchocki

President and founder of Eagle Associates, Inc., has over 42 years experience in marketing and consulting for the healthcare industry.
The primary objectives for this presentation includes:

- Understanding the process of auditing
- Understanding the relationship of HIPAA Rules, the HITECH Act, and the OMNIBUS Rule
- What have you attested to with a SRA for Meaningful Use
- What is the Security Rule requirement for a risk analysis
- How to conduct a Security Risk Analysis

This is your opportunity to ask all the HIPAA questions you can think of!
Auditing for Security

The Process of Auditing

- Identify or provide an explanation of what you are verifying or reviewing. For example, list the specific requirement in a regulation that you are reviewing to ensure compliance by your practice.
- Identify the location of written policies and procedures that you have developed and implemented in accordance with the regulation.
- Document and explain your findings. This should be simple statements that explain you found that your practice had fully implemented the written policy and therefore was in compliance with a specific requirement. Or, you might find that your practice is not met the requirement because a policy was either not written or not implemented.
- Explain corrective actions, if needed. This is a simple process of explaining what your actions will be to correct the deficiency or failure in compliance for specific requirement.
- Verify completion of any corrective actions. This can be as simple as documenting the date that the corrective action was implemented.
- Date your work. Without a specific date for the audit and corrective actions you may find regulators questioning the timeliness of your work.

Security Rule and HITECH Act

Security Rule

Scope of Information Covered

HHS stated in the February 20, 2003 posting of the Security Standard, as a general proposition, any electronic protected health information (EPIH) received, created, maintained, or transmitted by a covered entity is covered by this final rule. We agree that certain information, from which individual identifiers have been stripped (known as de-identified information), does not come into the purview of this final rule.
Security Rule Overview

Flexible and scalable standards
The security requirements were designed to be technology-neutral and scalable from the very smallest of provider practices, to the very largest of provider enterprises. Covered entities will find that compliance with the Security Rule will require an evaluation of what security measures are currently in place, as accurate and thorough risk analyses, and a series of documented solutions derived from a number of complex factors unique to each organization.

HHS recognizes that each covered entity is unique and varies in size and resources, and that there is no totally secure system.

From 45 CFR § 164.308(b):
Factors that must be considered:

- 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.

Meaningful Use Core Element #15

Eligible Professional
Meaningful Use Core Measures
Measure 15 of 15
Stage 1
Date issued: November 7, 2010

Protect Electronic Health Information

Objective
Prohibit electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

Measure
Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

Exclusion
No exclusion.
As mentioned previously the Security Rule contains standards and implementation specifications. These are organized into four areas of compliance:

- **Administrative Safeguards** are intended to provide the practice with administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures for electronic protected health information, and to manage the conduct of the practice’s workforce.

- **Physical Safeguards** are intended to provide the practice with physical measures, policies, and procedures to protect the practices electronic protected health information, building or facilities, and equipment.

- **Technical Safeguards** are intended to provide the technology, policies, and procedures for the use and protection of electronic protected health information in a practice’s information system. The Security Rule does not require specific technology solutions. There are many technical security tools, products, and solutions that practices can select from. Determination of specific security measures is up to each individual practice, based upon what is reasonable and appropriate for the size and complexity of the practice.

- **Organizational Requirements** address of practices capability for developing written policies and procedures, documentation and record keeping, maintenance of documentation for specified periods, availability of policies and procedures, and maintaining compliance with current regulatory requirements.
The process of conducting a risk analysis involves five critical steps.

1. First remember to date your work so you can prove when the analysis and corrective actions, if necessary, were completed.
2. Identify the item that you are analyzing or assessing. In the case of a risk analysis this should be the standard or specification that you are reviewing to ensure that your practice has met the requirements for compliance.
3. Identify the location of your policies and procedures. This is a simple reference in the risk analysis that identifies where to find applicable policies and procedures. For example, you may find that policies are included or controlled by your HR department, IT Department, or ideally collected in one location under the control of the Security Officer.
4. Document findings. This is a pretty straightforward step that will list for example, if you found that the appropriate policies and procedures were in place and implemented, or if you were to find a lack of compliance in the need to develop and implement appropriate corrective actions.
5. Document corrective actions. This step might also be known as implementing remedial actions or corrective actions that are intended to bring your practice into compliance with the guidelines provided in a standard or implementation specification.
The risk analysis begins with the first standard under administrative safeguards which is the security management process. This standard has four implementation specifications.

- **Risk Analysis** - The first specification is to conduct a risk analysis. This is an initial and periodic or subsequent analysis or assessment of the practice’s security processes to identify the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information that is collected and maintained by the practice. Documentation of the risk analysis, as with all HIPAA documentation, must be maintained for a minimum of six year. It is important to note that the risk analysis is not a onetime process - it should be completed annually.

- **Your finding for a Risk Analysis would be to list the date that the risk analysis was conducted.**

- **Risk Management** - While the risk analysis is the process of finding, the specification for risk management involves the process of developing and implementing appropriate corrective actions for any risks identified curing the risk analysis process.

- **Your finding for Risk Management would be to verify that appropriate corrective actions (if needed) were implemented by specific date or, in the case of strong compliance, that there were no corrective actions for this risk analysis.**

The requirement for sanction policy requires that your practice have written sanctions or penalties that would be applied when a workforce member fails to comply with the security policies and procedures that have been established by the practice. There are normally two locations for such policies, if they do exist in your practice. One location would be in your general HIPAA policy manual or in an employee handbook or HR policy. The number and severity of sanctions is at the discretion of the practice and can range from verbal reprimands, too written reprimands, to suspension from work, to termination of employment.

It is important for workforce members to have knowledge that sanctions will be imposed than what the sanctions are violations of security policies and procedures. This should be part of your practice’s new hire orientation training, annual training, and should be covered in a confidentiality agreement that is required for all workforce members to sign. The practice should ensure that sanctions, if imposed, are applied equally for all workforce members.

**The finding for Sanction Policy should identify that the practice does have existing sanctions that would be imposed for violating privacy, breach notification, and security policies and procedures of the practice. Be sure to identify the location of the policies such as if they are in an employee handbook, HR policies, or general HIPAA policies.**
The requirement for Information System Activity Review is intended to provide the practice with the ability to monitor and identify inappropriate access, or use or disclosure of electronic protected health information from the practice's information system. The policy and procedure for this specification should help the practice identify, track, or document under authorized activities in the information system. While large organizations and institutions might use automated programs, this is more of a periodic or as-needed process in most practice settings. The use of audit logs, access reports, and security incident tracking will be a few of the tools utilized to meet this requirement.

Your finding for the Information System Activity Review would be to verify that the Security Officer or another designated individual in the practice has the capability to perform these functions.

The requirement for assigned security responsibility requires a practice to designate a single person (security officer) who will be responsible for the development and implementation of policies and procedures as required by the security room. While there is one individual designated as the security officer, they may be assisted by a group or committee.

The finding for assigned security responsibility should identify who has been assigned the role of security officer.
The requirement for workforce security involves three addressable specifications. The objective is to ensure that all workforce members have appropriate access to the electronic protected health information and that policies and procedures prevent unauthorized access.

The specification for authorization and/or supervision is the process of determining whether a particular user of the practice’s information system has been granted the authority or right to carry out a certain activity, such as reading a file or running a program. Implementation of this specification will vary among covered entities, depending upon the size and complexity of the workforce in the information system that contains electronic protected health information.

The finding for the specification would identify the types of access that are granted to workforce members such as global authorization (as found in smaller practices) or role-based authorizations for users of the information system. You should also identify the individual, such as the Security Officer, in your practice that has the administrative ability to assign, monitor, and control access to the information system.

The specification for workforce clearance procedures ensures that the access of an authorized user of the practice’s information system is appropriate for their role or job title in the practice. There should also be a screening process in place for new hires and outside entities that may be assigned access to the practice’s information system.

The method that a practice uses to screen new hires and outside entities will vary from simple reference checks, to complex background investigations. Note that the requirement does not specify any particular method. At a minimum, a practice should check references on all new hires and entities along with performing a check of the OIG exclusionary database for fraud and abuse listings. Using the OIG database helps accomplish clearance procedures and simultaneously meets the requirement from the OIG to check individuals against their database.

The finding for workforce clearance procedures should identify that the practice does have appropriate policies and procedures for workforce clearance prior to assigning authorized access to the information system. A practice should check references for all new hires and check their identity against the OIG exclusionary database (this OIG check should be repeated, at a minimum, annually for all workforce members.)
The specification for termination procedure requires the practice to have implemented a policy and procedure that ensures the deactivation of the user’s ID for accessing electronic protected health information and the collection of any physical means of accessing the facilities of the practice (such as collecting keys, changing combination locks, collecting access cards, changing alarm codes, etc.).

The finding for termination procedure should include a note that indicates who in the practice has the responsibility for terminating electronic access to electronic protected health information and collecting means of physical access to the facilities of the practice.

Documentation of the termination process for workforce members and outside entities that have had their access terminated should be maintained and available for review for a minimum of six years.

The standard for information access management as three implementation specifications.

The requirement for isolating clearinghouse functions is actually the responsibility of the clearinghouse used by the practice if the clearinghouse is owned by a larger organization. The purpose of this specification is for the practice to obtain satisfactory assurance, through the use of a business associate agreement, that the use and disclosure of electronic protected health information, as provided to the clearinghouse by the practice, is limited to the contracted services of the clearinghouse and that the information will not be used or disclosed by the larger organization, if one exists.

The finding for isolating clearinghouse functions is that the practice does have a business associate agreement with the clearinghouse. The agreement might also be with a larger organization and specifies the isolation of information from a larger organization.
The specification for access authorization requires that you have written policies and procedures identifying how access to your information system is assigned or authorized for workforce members and outside entities. Authorization is defined as the act of determining whether or not a particular user has the right, based on job functions or responsibilities, to carry out a certain activity, such as reading a file or running a program in the information system.

The finding for access authorization should identify that the practice does have a process or procedure in place to grant and control access to its information system.

The specification for access establishment and modification is the documentation component to access authorization. The practice should maintain documentation that identifies assignment of user ids (for example who the user id has been assigned to), the date of establishment or assignment, the dates and details of any modifications up to an including termination from the information system. Note that many EHR systems now have the capability of producing such documentation for the practice. If not, the practice should maintain a log or record.

The findings for access establishment and modification should identify that the practice does have such documentation, who has the responsibility for maintaining it, and that there is an ability to retrieve such information.

The specifications for security awareness and training is intended to ensure that all workforce members, including management, are aware of security issues and are adequately trained to help ensure the protection of electronic protected health information.

The specification for security reminders requires a practice to provide periodic security reminders for workforce members. Reminders can include notices or memos in electronic or printed form, agenda items are topics discussed at periodic staff meetings, posted reminders on bulletin boards, and retraining for specific security policies and procedures. Note that this type of reminder should be included as part of new hire training in annual security training.

The finding on this specification should indicate that the practice does use security reminders and briefly explain the process used in work samples and documentation can be located in the practice.
The specification for protection from malicious software is a requirement for the practice to raise awareness for malicious software and communicate the role of workforce members in protecting the information system. Malicious software can be thought of as any program that harms information systems, such as viruses, Trojan horses or worms. As a result of an unauthorized infiltration, electronic protected health information and other data can be damaged or destroyed, and at a minimum, require expensive and time-consuming repairs. Malicious software is frequently brought into an organization through email attachments, programs that are downloaded from the Internet.

The specification for login monitoring requires a practice to make workforce members aware of the need to monitor login attempts and the responsibility to report discrepancies, alert messages, or other unusual behavior when logging into the information system.

The specification for password management is intended to remind and make workforce members aware of the need to guard not only their password but user ID to the information system. Be aware that many workforce members may not understand that the use of their user ID and password leaves a trail identifying all activities either by them or another individual in the information system.

The findings for these three specifications should indicate that there is training and awareness for each topic and that it is provided upon hire into the practice and annually thereafter as part of the practice’s security training program.

The Standard for security incident procedures has one specification requires a practice to implement procedures for handling and documenting “security incidents” and the resolution to such incidents. A security incident is defined as an attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in the practice’s information system.

The specification for response and reporting of security incidents requires a practice to implement a system for handling such incidents. Addressing security incidences as an integral part of the overall security program for the information system. Whether or not a specific occurrence or incident is considered a security incident, the process of documenting all incidents, what information should be contained in the documentation, and what the appropriate response should be will be dependent upon the practice’s environment and the information involved in the incident.

A practice should be able to rely upon the information gathered in complying with the other Security Rule standards (for example it’s risk assessment, risk management procedures, and privacy standards) to determine what constitutes a security incident, in the context of its business operations.

The finding for this specification should identify that the practice and its workforce members are aware of what would be considered potential security incidents, who to report such incidents to, and the documentation of any investigation and corrective action performed by the practice.
The standard for a contingency plan as five specifications. A contingency can be defined as a future event or circumstance that is possible but cannot be predicted with certainty such as an emergency or disaster that might occur and require restoration of the practice’s information system. A worst-case scenario could include a practice burning to the ground or being wiped out by a severe weather events such as tornadoes, hurricanes, and flooding. So, a contingency plan could also be defined as what will your practice do, in the event of an emergency, to ensure the integrity and availability of patient information and continued operations to serve patients the practice.

The specification for a data backup plan requires some practice to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information that it has collected, created, and maintains on its patients. Data backup can vary from practice to practice using either local backup (such as tape or other local drive back up) or cloud service or other remote devices. A critical element is to ensure that your backup data is stored off-site from the practice. This will ensure its availability in the event of a black hole situation for the information system.

The finding for the specification would identify that the practice does have a system for backing up its data, that the data is stored off-site, and that it is secure (i.e., encrypted or secured by other means). This is a specification that should include detailed operating procedures identifying how the backup process is achieved, the location of the stored data, the security for the stored data, and the means for retrieving and using the backup data to restore the information system.

The specification for disaster recovery plan requires a practice to have plans and procedures to recover and restore data in the case of any disaster. The timeliness of the actions in this specification will be somewhat dependent upon the disaster or emergency as well as the specifications for emergency mode operations and application and data criticality analysis will play a role in determining the restoration of the practice’s information system. One of the critical elements for disaster recovery plan would include identifying the hardware and applications that would be needed to restore or rebuild the information system in the event of an emergency or disaster.

The finding for this specification should include identifying that a listing of assets for the information system is maintained (both on-site and off-site) to ensure availability for its use.

The specification for emergency mode operations requires a practice to address how it will continue to operate and serve patients in the event of an emergency or disaster. An emergency can range from a power outage or blackout to natural disasters such as hurricanes, tornadoes, and earthquakes. Emergency mode operations will also be dependent upon the length of time that the emergency or disaster will be affecting the information system.

The finding for the specification should list options for the practice and its ability to serve patients in the event of an emergency or disaster. This could include closing the practice until power is restored in the information system is operating again, choosing to continue serving patients in a paper-based mode until the information system is restored and then entering data at that time. The possibility of operating from a remote location, or the use of the backup generator system that would require verifying the integrity of your data prior to continuing operations utilizing the generator system.
The specification for testing and revision requires a practice to review the elements of its contingency plan to ensure that it is still viable and includes current technical capabilities, environmental considerations, and current regulatory requirements. This requirement can be accomplished by conducting an annual risk analysis which would include reviewing and revising, if necessary, elements of the contingency plan.

The finding for the specification could be as simple as stating that the elements of the contingency plan are reviewed on an annual basis as part of the practice’s annual risk analysis process.

The specification for application and data criticality analysis should identify what software applications and data from the information system would be critical to continuing operations in the event of an emergency or disaster or significant problem with the information system. Meeting this requirement could include options that were discussed under emergency mode operations.

The finding for this specification should identify the applications and data that would need to be available to the security officer and management personnel in the event of an emergency or disaster or significant problem with the information system.

Evaluation is both the standard and a specification requiring the practice to periodically evaluate and determine if its security policies and procedures continued to provide protection for electronic protected health information. This is accomplished through ongoing monitoring and evaluation of the practice’s environment, technical capabilities, and regulatory requirements. Conducting an annual risk analysis will enable a practice to meet this requirement.

The findings for this specification should indicate how the practice periodically evaluates security policies and procedures. As stated, conducting an annual risk analysis will ensure proper monitoring and evaluation for this requirement.

The requirement for business associate agreements is again both a standard and a specification. A practice is expected to maintain business associate agreements with persons and entities that fit that description as required by the Privacy Rule and now, again, for security. The 2013 Omnibus Rule required modifications or updates to existing business associate agreements. The security officer or individual with responsibility in the practice for maintaining such agreements should ensure that updates were made in accordance with 2013 changes.

The findings for this standard should indicate that the practice does have business associate agreements with persons or entities that fit that description, who is responsible for maintaining the agreements, and the location of the agreements.
As mentioned previously, physical safeguards are intended to provide the practice with physical measures, policies, and procedures to protect the practice's electronic protected health information, building or facilities, and equipment.

The standard for facility access controls has four specifications that require a practice to develop and implement procedures for securing the physical facility for its practice.

The specification for contingency operations is fairly straightforward in that it requires a practice to identify individuals or entities that would require access to the practice's facility to assist in restoration or rebuilding of the information system in the event of an emergency or disaster. This could be accomplished by creating a list or allowing the security officer in management personnel for the practice to identify appropriate personnel they would deem necessary to have access to the facility in the event of an emergency or disaster.

The finding for the specification should identify how the practice will restore or continue operations and who would be needed to assist in that effort.

The specification for facility security plan will ensure that only authorized personnel will have access to the practice's facility and equipment that contains electronic protected health information. Documentation of who will have access will be accomplished in the next specification. This specification also requires a practice to identify how it's will secure its facility. The findings for the specification should indicate how the facility is secured. Examples would include the use of key locks, combination locks, pass cards, alarm codes, and other means for controlling physical access.

The specification for access control and validation would be the documentation portion of the practice's facility security plan. The findings for this specification would indicate how the practice assigns means of access to the facility and controls her maintains accountability for assignment of keys, codes or other means of access.

The specification for maintenance records requires that a practice maintain a system for documenting modifications or maintenance affecting means of access to the facility. For example, this would include documenting changing key locks, alarm codes or other means of access to the facility and, in the event that the information is secured in a separate room, modifications for access to that location.

The finding for this specification should be that the practice maintains or (if there has been no maintenance) will maintain appropriate documentation.
The standard for workstation use and security relates to the physical location, surroundings, and use of workstations and other devices that can access and/or store electronic protected health information. This would include evaluation for desktop computers, laptops, tablets, exam room terminal screens, smart phones, PDAs, laboratory analyzers, EKG machines, and other such devices that are capable of either accessing or storing patient information. Another consideration for this specification comes into play when the practice has workforce members that operate from remote locations to include homes. Concerns to address in this specification include:

- Has staff been instructed on the proper use of their workstations and the need to limit access by non-workforce members?
- Has staff been instructed on the location and placement of computer screens to only allow clear viewing by authorized individuals?
- As the practice implemented the use of password-protected screen savers and/or automatic log off in areas where devices might be left unattended and accessible to unauthorized personnel?
- At workstation security policies and procedures been implemented with staff that work remotely, have access to, or work with devices storing electronic protected health information?
- At physical safeguards such as limited access areas been identified to prevent use of workstations by unauthorized personnel?
- Have all types of workstations with access to, or storage of electronic protected health information been identified?
- Is there a need to implement additional measures to ensure the physical safeguard for workstations?

The findings for this standard will be determined by answers to these questions.

The standard for device and media controls has four specifications. The objective is to implement policies and procedures that control the receipt and removal of hardware and electronic media, that contain electronic protected health information, into and out of the practice, and the movement of devices and media within the facility. As referenced here, the term “electronic media” means, electronic storage media including memory devices and computers and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. This standard covers the proper handling of electronic media including receipt, removal, backup, storage, reuse, disposal and accountability.

The specification for disposal requires that your practice have policies and procedures to ensure that electronic protected health information is securely removed from devices (includes devices such as digital copy/fax machines) and media or that the device or media is sufficiently damaged beyond repair, making the data inaccessible.

The findings for this specification should identify how your practice properly disposes of media and devices. The security officer should maintain a record of electronic media disposal that demonstrates requirements have been met.

The specification for media reuse requires policies and procedures governing the reuse electronic media rather than its disposal. Whether electronic media is reused within the practice, or outside, it is important to remove all electronic protected health information stored on the media to prevent unauthorized access to patient information. Internal reuse may include redeployment or sharing of media such as flash drives, CDs, DVDs, tapes, etc. External reuse may include donation of electronic media to charity organizations, schools or, in some cases, resale to employees or others.

The findings for this specification will be determined based on whether or not your practice does reuse electronic media.
HIPAA Auditing - Security Risk Analysis

Physical Safeguards
STANDARD - Device and Media Controls
* Disposal
* Media Reuse
* Accountability
* Data Backup and Storage

The specification for accountability is only applicable if the practice moves devices (that store electronic protected health information) to locations other than the primary facility. Other locations would include satellite offices as well as homes of staff or other workforce members. This specification does not apply to portable devices such as laptops or tablets that are moved from, and consistently return to, the primary facility.

The findings for this specification will depend upon these questions
* Does the practice relocate devices that store electronic protected health information?
* If yes, is there documentation that tracks the relocation for such devices?

The specification would be not applicable if your practice is not relocate such devices.

The specification for data backup and storage requires a practice, prior to moving devices that store electronic protected health information, to back up such data for restoration on the device in the event that the original data were damaged or it’s integrity was questioned due to the movement.

The finding for this specification is dependent upon whether or not your practice does move devices.

As mentioned previously, technical safeguards are intended to provide the technology, policies, and procedures for the use and protection of electronic protected health information in a practice's information system. The Security Rule does not require specific technology solutions. There are many technical security tools, products, and solutions that a practice can select from. Determination of specific security measures is up to each individual practice, based upon what is reasonable and appropriate for the size and complexity of the practice.

The standard for access control has four specifications. The practice must implement technical policies and procedures that allow access to the information system and electronic protected health information only by those persons that have been granted access rights, as specified in the Security Rule. This requirement relates to the administrative safeguards on access authorization and access establishment and modification.

The specification for unique user identification requires a practice to ensure that each user of the information system as a unique identifier to access the system. A practice should assign a username and password for each workforce member, technical support personnel, and outside entities who will have access to the information system. The security officer should ensure that all user IDs are unique and are not shared.

The findings for this specification should indicate that each workforce member has been assigned a unique user identifier and that this identifier can be used to track user activity within the information system.
The specification for emergency access procedure requires a practice to establish procedures for obtaining necessary electronic protected health information during an emergency or disaster. The security officer should identify the persons who will be responsible for restoring access in such cases. The designated individuals will be responsible for determining how access to information will be gained in the event that normal environmental systems, such as electrical power, are in operable due to a natural or man-made emergency or disaster.

The findings for this specification should identify that the security officer has established persons and/or outside entities that may be necessary to assist in restoring access to information in the information system in the event of an emergency or disaster.

The specification for automatic log off requires that a practice implement electronic or, as an alternative method, manual termination of an electronic session after a predetermined time of inactivity, or at the end of the day.

The findings for the specification should identify the practices method for meeting the requirement for automatic log off or the practices use of an alternative method such as manual termination of electronic sessions.

The specification for encryption/decryption requires a practice to implement a method or mechanism to encrypt and decrypt electronic protected health information. This is especially critical for backup data and portable devices or media that store such information.

The findings for this specification should identify that the practice has inventory and identified devices and media requiring the use of encryption to protect patient information.

The standard for audit controls requires that a practice implement mechanisms that will record and allow tracking of user activities within the information system. EMR systems may provide the practice with the ability to audit, track, and produce documentation of user activity. For most practices use aquatic controls and reports will function as an investigative tool that enables the practice to determine unauthorized and inappropriate use of electronic protected health information within the information system.

The findings for this specification will be determined by the ability of the practice or security officer and their understanding of functions within the EMR system that provided capability for auditing activities of individual users in the information system.
The standard for integrity and mechanism to authenticate is met by implementing electronic mechanisms to confirm that electronic protected health information has not been accessed or altered or destroyed in an unauthorized manner.

Integrity is defined in the Security Rule as the indication that data or information has not been altered or destroyed in an unauthorized manner. Protecting the integrity of electronic protected health information is one of the primary goals of the Security Rule. Information that has been improperly altered or destroyed can result in clinical quality problems for the practice, including patient safety issues. The integrity of data can be compromised by both technical and non-technical sources. Workforce members or business associates of the practice may make accidental or intentional changes that improperly alter or destroy information in the practices system. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures.

Methods to protect data integrity and the physical environment include: making server successful only to network administrators, keeping transmission media such as cables and connectors covered and protected to ensure they cannot be tapped, and protecting hardware and storage media from power surges, electrostatic discharges, and make magnetism.

The findings for the specification will be determined by the practice’s ability to control access to electronic protected health information and prevent unauthorized alteration or destruction of patient information.

The standard for person or entity authentication requires a practice to implement procedures that will verify a person or entity seeking access to electronic protected information is who they claim to be. In general, authentication ensures that a person is, in fact, who he or she claims to be prior to allowing access to information. This is accomplished by providing proof of identity. There are several basic ways to provide proof of identity for authentication purposes.

- Requiring the use of a unique user ID within established password or PIN.
- Requiring individuals to use a smart card, a token, or key for access to information.
- Requiring something unique to the individual such as biometrics. Examples of biometrics include electronic recognition of fingerprints, voice patterns, facial patterns, or iris patterns.

Most practices will utilize one of the first two methods for authentication to access their information system. If authentication credentials entered into the information system match those stored in the system, the user will be authenticated and provided access to the information system.

The findings for this specification will identify that the practice has established appropriate policies and procedures for authentication of users attempting to access the information system.
The requirement for sanction policy requires that your practice have written sanctions or penalties that would be applied when a workforce member fails to comply with the security policies and procedures that have been established by the practice. There are normally two locations for such policies, if they do exist in your practice. One location would be in your general HIPAA policy manual or in an employee handbook or HR policy. The number and severity of sanctions is at the discretion of the practice and can range from verbal reprimands, too written reprimands, to suspension from work, to termination of employment.

It is important for workforce members to have knowledge that sanctions will be imposed than what the sanctions are violations of security policies and procedures. This should be part of your practice’s new hire orientation training, annual training, and should be covered in a confidentiality agreement that is required for all workforce members to sign. The practice should ensure that sanctions, if imposed, are applied equally for all workforce members.

The finding for Sanction Policy should identify that the practice does have existing sanctions that would be imposed for violating privacy, breach notification, and security policies and procedures of the practice. Be sure to identify the location of the policies such as if they are in an employee handbook, HR policies, or general HIPAA policies.

HIPAA Auditing - Security Risk Analysis
Organizational Requirements
STANDARD - Policies and Procedures
STANDARD - Documentation
STANDARD - Availability
STANDARD - Updates

The standard for policies and procedures requires a practice to develop and implement reasonable and appropriate policies and procedures in compliance with the standards, implementation specifications, or other requirements of the Security Rule. While this standard requires a practice to develop and implement written policies and procedures, it does not define either “policy” or “procedure”. Generally, policies define a practice’s intent to comply with the requirement within a regulation. Procedures describe the methods that practice will use to fulfill, or comply with the policy. The findings for this standard should indicate the existence of required policies and procedures.

The standard for documentation has three requirements. A practice must maintain policies and procedures in written or electronic form. A practice must maintain written or electronic documentation for actions, activities, or assessments required by the Security Rule. A practice must retain HIPAA related documentation for a minimum of six years from the date of its creation, or the date when it was last in effect, whichever is later. The findings for this standard will be based upon a practice’s ability to confirm meeting the three requirements.

The standard for availability requires a practice to make documentation available to those persons or entities responsible for implementing the policies and procedures to which the documentation pertains. The findings for this standard should confirm that policies and procedures are available for implementation and review.

The standard for updates requires that a practice periodically review policies and procedures and, as needed, update them to reflect changes in regulatory requirements or the operational characteristics of the practice affecting the security of electronic protected health information. The findings for this standard should confirm that the practice has appropriately maintained and updated security policies and procedures.
“A Security Risk Analysis is More Than Meaningful Use

An Eagle Associates Presentation
Eagle Associates, Inc.
www.eagleassociates.net
P.O. Box 1356
Ann Arbor, MI 48106
800-777-2337