UTZ & MILLER LLC
ATTORNEYS AT LAW

APRIL 5, 2005 VOLUME 1, NUMBER 7

*"The purpose of the Security Rule is to provide national standards for safeguards to protect the confidentiality, integrity, and availability of 'electronic protected health information' ('EPHI')."*

# COMPLIANCE WITH THE HIPAA SECURITY RULE

**By**
**Matthew J. Eickman**
**Utz & Miller, LLC**
**(913) 685-0749**
**meickman@utzmiller.com**

When you sent out your company's Privacy Notices on or around April 14, 2003, and set into motion procedures for complying with the HIPAA Privacy Rule, you may have thought you had crossed every major HIPAA Compliance hurdle. But the chances are that your company has more work to do and it may need to act soon. An April 20, 2005 deadline for complying with another set of HIPAA Standards – the HIPAA "Security Rule" – is fast-approaching for many covered entities. Naturally, when you hear the terms "HIPAA" and "Security Rule," many questions may run through your mind. For example, what is the Security Rule? Are my company's plans subject to the Security Rule? If so, when must the plans comply? What steps are required?

There are short answers to those questions, but they are not that helpful. For instance, what does it mean to say that the Security Rule adopts national standards for safeguards to protect electronic protected health information? Also, what does it mean to say that a covered entity must implement policies and procedures to ensure it complies with the Security Rule's safeguards, standards, and implementation specifications?

Please use the information below to answer some of those questions and to begin taking the steps necessary for your health plans to comply with the Security Rule.

## WHAT IS THE SECURITY RULE?

**Background.** Prior to HIPAA, there were no generally accepted security standards or general requirements for protecting health information in the health care industry. Yet, as technologies evolved, the health care industry began to move away from paper processes. It started to rely more heavily on computers to pay claims, answer eligibility questions, provide health information, and conduct many other administrative and clinically-based functions. As a result of those changes, the confidentiality of health-related information has become threatened not only by the risk of improper access to stored information, but also by the risk of interception during electronic transmission of the information.

The purpose of the Security Rule is to provide national standards for safeguards to protect the confidentiality, integrity, and availability of "electronic protected health information" ("EPHI"). Those standards generally require measures to be taken to secure EPHI both while it is being stored by covered entities as well as while it is being transmitted.

*"A plan with more than $5 million in annual receipts (more than $5 million in annual premiums for an insured plan or in total annual claims for a self-insured plan), . . . must comply with the Security Rule by April 20, 2005."*

**Utz & Miller, LLC**
13200 Metcalf
Suite 230
Overland Park, KS 66213

Phone: 913.685.0970
Fax: 913.685.1281

**John L. Utz**
jutz@utzmiller.com
Phone: 913.685.7978
Fax: 913.685.1281

**Eric N. Miller**
emiller@utzmiller.com
Phone: 913.685.8150
Fax: 913.685.1281

**Matthew Eickman**
meickman@utzmiller.com
Phone: 913-685-0749
Fax: 913.685.1281

www.utzmiller.com



**General Requirements**. As we will discuss later in this newsletter, the Security Rule imposes several specific requirements on your health plans (and other covered entities). It may be easier to understand and satisfy those requirements if one considers the Security Rule's general obligations. First, your health plans must ensure the **confidentiality, integrity, and availability** of all EPHI your plans create, receive, maintain, or transmit. Second, your plans must **protect against any reasonably anticipated threats or hazards** to the security or integrity of that EPHI. Third, your plans must **protect against any reasonably anticipated uses or disclosures** of that information that are not permitted or required under the Security Rule. Fourth, you must ensure that your **workforce complies** with the Security Rule.

**Scope**. The scope of the information protected by the Security Rule is narrower than that of the HIPAA Privacy Rule. You may remember that the Privacy Rule addresses privacy protections for "protected health information" or "PHI," which is individually identifiable health information that is transmitted by or maintained by a health plan (or other covered entity), subject to three exceptions. In other words, PHI is health information that could be used to identify a particular individual. The definition of PHI is broad, in that it includes health information transmitted or maintained by electronic media *or in any other form or medium*. The Security Rule, however, addresses privacy protection only for a narrower subset of PHI – "electronic PHI" or "EPHI." EPHI includes only PHI that is transmitted by or maintained in electronic media.

Thus, there may be some health information that is protected under the Privacy Rule, but is not protected under the Security Rule. Further, it is important that PHI must have existed in an electronic form prior to its transmission or be stored in electronic form in order for it to be EPHI and, as a result, for it to be protected by the Security Rule. For example, because paper-to-paper faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by the Security Rule.

## Is My Plan Subject to the Security Rule?

The Security Rule, like the Privacy Rule, applies to a "covered entity," which is defined as one of the following:

(1) a health plan;
(2) a health care clearinghouse; or
(3) a health care provider that conducts any standard transactions electronically, or that engages third parties to process those transactions electronically.

A "health plan" is an individual or group plan that provides or pays the cost of medical care. This definition includes nearly all arrangements that pay the cost of medical care, including, for example, group health plans, dental plans, some employee assistance plans, and HMOs. This definition also includes health care flexible spending accounts (including those offered through a cafeteria plan) used to reimburse employees for medical expenses. A plan with fewer than 50 participants that is self-administered by the employer that established and maintains the plan, however, is excluded from the definition of "health plan." That exclusion typically will apply to flexible spending accounts that have fewer than 50 participants and are not administered by a third-party administrator.

It is your company's *health plans'* EPHI – not your company – that is subject to the Security Rule. As a practical matter, however, your company will be responsible for its sponsored health plans' compliance with the Security Rule.

*"A covered entity, such as an employer's health plan, must assign final responsibility for the entity's security to one official – the 'Security Official.'"*

**Utz & Miller, LLC**
13200 Metcalf
Suite 230
Overland Park, KS 66213

Phone: 913.685.0970
Fax: 913.685.1281

**John L. Utz**
jutz@utzmiller.com
Phone: 913.685.7978
Fax: 913.685.1281

**Eric N. Miller**
emiller@utzmiller.com
Phone: 913.685.8150
Fax: 913.685.1281

**Matthew Eickman**
meickman@utzmiller.com
Phone: 913-685-0749
Fax: 913.685.1281

www.utzmiller.com



## WHEN MUST A COVERED ENTITY COMPLY WITH THE SECURITY RULE?

Like the Privacy Rule, the Security Rule imposes a general compliance deadline and a special, later deadline on small plans. A plan with more than $5 million in annual receipts (more than $5 million in annual premiums for an insured plan or in total annual claims for a self-insured plan), health care clearinghouse, or health care provider must comply with the Security Rule by April 20, 2005. A small plan (one with $5 million or less in annual premiums or claims) has until April 20, 2006, to comply with the Security Rule.

Your work under the Security Rule is not finished just because you meet the initial deadline. The Security Rule requires, instead, that security measures implemented to comply with the Security Rule be reviewed and modified as needed to continue provision of reasonable and appropriate protection of Electronic PHI. The Centers for Medicare and Medicaid Services ("CMS") explains: "Security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entities' organizations and technologies change."

## WHAT STEPS DO I NEED TO TAKE?

As we discussed above, the Security Rule provides four overarching requirements and several specific requirements. If you have responsibility for your company's health (or cafeteria) plans, you need to be aware of the following specific Security Rule requirements:

- **Appoint a security official;**
- **Conduct a risk analysis;**
- **Amend group health plans (including health care flexible spending accounts offered through cafeteria plans);**
- **Amend business associate agreements;**
- **Adopt written policies and procedures; and**
- **Ensure your workforce complies with the Security Rule.**

**Appoint a Security Official**. A covered entity, such as an employer's health plan, must assign final responsibility for the entity's security to one official – the "Security Official." The Security Official will must also be the one who is responsible for the development and implementation of the policies and procedures required by the Security Rule. The same person may serve as both the HIPAA Security Official and the HIPAA Privacy Official.

**Conduct Risk Analysis**. A health plan (or other covered entity) is required to conduct a risk analysis. More specifically, the Security Rule requires that this be an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity. The results of this risk analysis will impact the manner in which your health plans comply with the Security Rule. Thus, it is important that this step be taken *before* adopting written policies and procedures, and implementing those policies and procedures. This is because the Security Rule, while rigid in many respects, provides a certain amount of flexibility.

The drafters of the Security Rule recognized that covered entities vary in a wide range of characteristics and that no single inflexible set of security standards would fit for all of those entities. As a result, the Security Rule gives a health plan the discretion to use any security measures that allow it to reasonably and appropriately implement the Rule's required standards and implementation specifications. For example, a health plan (or other covered entity) must take into account its size, complexity, capabilities, technical infrastructure, hardware, and software capabilities. Also, it must take into account the costs of security measures and the probability and criticality of potential risks to EPHI.

*"If your company sponsors a 'group health plan,' the plan document must be amended so that it provides that the plan sponsor (typically, your company) will reasonably and appropriately safeguard EPHI . . .."*

All of those flexible factors may be explored through a risk analysis. The results of the risk analysis will impact the policies and procedures your plans implement (as discussed later in the "Adopt Written Policies and Procedures" section). We suggest the risk analysis be conducted as soon as possible so that your plans may best take advantage of the Security Rule's provided flexibility, and develop policies and procedures that best suit your plans' individual characteristics. In other words, your plans should conduct their risk analysis as far in advance of the April 20, 2005 (or 2006, if applicable) deadline as practical.

**Amend Plans**. If your company sponsors a "group health plan," the plan document must be amended so that it provides that the plan sponsor (typically, your company) will reasonably and appropriately safeguard EPHI created, received, maintained, or transmitted to or by your company on behalf of the group health plan. A group health plan is a plan that provides medical care to employees or their dependants directly or through insurance, reimbursement, or otherwise. Thus, for example, not only must your medical plan be amended, but also your cafeteria plan must be amended if that plan includes flexible spending accounts used to reimburse employees for medical expenses.

This plan amendment must include provisions that require your company, as the plan sponsor, to do the following:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI it creates, receives, maintains, or transmits on behalf of the group health plan;
2. Ensure that the adequate separation between the company and the group health plan (as required by the Privacy Rule) is supported by reasonable and appropriate security measures;
3. Ensure that any agent, including a subcontractor, to whom the company provides EPHI created, received, maintained, or transmitted on behalf of the plan, agrees to implement reasonable and appropriate security measures to protect that information; and
4. Report to the group health plan any security incident of which the company becomes aware.

Like the previously required Privacy Rule plan amendment, there is an exception to the Security Rule plan amendment obligation when there will be limited sharing of EPHI between a plan and a plan sponsor. If your health plan will share with your company only "summary health information," and plan enrollment and disenrollment information, the plan need not be amended.

If that exception does not apply to your health plan, note that these required changes are not merely changes to the plan document, but also require your company to take significant actions. Your company must implement the protective safeguards and ensure that adequate separation is supported by adequate security measures. It must enter into an agreement with agents with which the company will share the plan's EPHI. Also, if your company becomes aware of the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information (a "security incident"), it must report that activity to the plan.

**Amend Business Associate Agreements**. The Privacy Rule required that covered entities enter into agreements with their "business associates," and the Security Rule requires amendments to these agreements. You may remember that a business associate is an entity that performs a function or activity on behalf of a covered entity or provides certain specific services for a covered entity, and has disclosed to it individually identifiable health information. Examples of health plans' business associates are third party administrators and, in many circumstances, insurance brokers or actuarial consultants.

**Utz & Miller, LLC**
13200 Metcalf
Suite 230
Overland Park, KS 66213

Phone: 913.685.0970
Fax: 913.685.1281

**John L. Utz**
jutz@utzmiller.com
Phone: 913.685.7978
Fax: 913.685.1281

**Eric N. Miller**
emiller@utzmiller.com
Phone: 913.685.8150
Fax: 913.685.1281

**Matthew Eickman**
meickman@utzmiller.com
Phone: 913-685-0749
Fax: 913.685.1281

www.utzmiller.com

*"The Security Rule requires that . . . business associate agreements be amended."*

The Security Rule requires that these business associate agreements be amended. The agreements must be changed so they require the business associate to:

1. 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 covered entity as required by the Security Rule;
2. Ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect it;
3. Report to the covered entity any security incident of which it becomes aware; and
4. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

**Adopt Written Policies and Procedures**. The bulk of the Security Rule describes requirements (called safeguards, standards, and implementation specifications) with which a health plan (or other covered entity) must comply. The Security Rule also requires that a covered entity adopt and implement *written* policies and procedures through which it will meet those requirements. The Security Rule includes a matrix of the required safeguards, standards, and implementation specifications. We have prepared a more detailed grid that includes the information from the Security Rule's matrix, with instructions for implementing the required standards and implementation specifications. The following discussion will provide you with background that will help in understanding that grid, which is attached at the end of this newsletter.

The Security Rule requires that covered entities adopt three broad categories of **Safeguards:** Administrative, Physical, and Technical. Each set of those Safeguards requires that a number of **Standards** be met. The Security Rule provides **Implementation Specifications**, which provide additional detailed instructions for implementing the Standards.

As you will see on the attached grid, some of the Implementation Specifications are **"Required"** while others are merely **"Addressable."** If one is "Required" by the Security Rule, a covered entity must implement policies and procedures that meet the Implementation Specification. If, however, one is "Addressable," a covered entity must access whether a given addressable Implementation Specification is a reasonable and appropriate security measure to apply within its particular framework. If a covered entity determines that an addressable Implementation Specification is not a reasonable and appropriate answer to its security needs, a covered entity must do one of two things: (i) implement another equivalent measure if reasonable and appropriate, or (ii) if the standard can otherwise be met, the covered entity may choose to not implement the Implementation Specification or any equivalent alternative measure at all. If a covered entity chooses to do one of these two things, it must document the decision not to implement the addressable specification, the rationale behind that decision, and either the alternative safeguard implemented to meet the standard or the way in which the standard is being otherwise met.

**Ensure Your Workforce Complies**. Your workforce will have to be trained to comply with your company's adopted policies and procedures. Because this may take some time, we suggest your company begin planning this training as soon as possible.

**Utz & Miller, LLC**
13200 Metcalf
Suite 230
Overland Park, KS 66213

Phone: 913.685.0970
Fax: 913.685.1281

**John L. Utz**
jutz@utzmiller.com
Phone: 913.685.7978
Fax: 913.685.1281

**Eric N. Miller**
emiller@utzmiller.com
Phone: 913.685.8150
Fax: 913.685.1281

**Matthew Eickman**
meickman@utzmiller.com
Phone: 913-685-0749
Fax: 913.685.1281

www.utzmiller.com

## CONCLUSION

The April 20, 2005 deadline for HIPAA Security compliance is fast-approaching for most health plans, health care clearinghouses, and health care providers. Plan sponsors and covered entities should act immediately to analyze risks and appoint a security official. They also should begin to amend plans and business associate agreements, train employees to comply with the Security Rule, and adopt and implement written plans and procedures.

**Utz & Miller, LLC**
13200 Metcalf
Suite 230
Overland Park, KS 66213

Phone: 913.685.0970
Fax: 913.685.1281

**John L. Utz**
jutz@utzmiller.com
Phone: 913.685.7978
Fax: 913.685.1281

**Eric N. Miller**
emiller@utzmiller.com
Phone: 913.685.8150
Fax: 913.685.1281

**Matthew Eickman**
meickman@utzmiller.com
Phone: 913-685-0749
Fax: 913.685.1281

www.utzmiller.com

# HIPAA SECURITY STANDARDS MATRIX

*The HIPAA Security Rule (45 C.F.R. Parts 160 and 164, Subpart C) requires that covered entities adopt three categories of safeguards: **Administrative**, **Physical**, and **Technical**. Each set of safeguards includes a number of **Standards**, and the Security Rule includes **Implementation Specifications**, which are additional detailed instructions for implementing those Standards. If an Implementation Specification is "**Required**," a covered entity must implement policies or procedures that meet the Specification. If, however, it is "**Addressable**," a covered entity must assess whether it is a reasonable and appropriate safeguard in the entity's environment.*

## ADMINISTRATIVE SAFEGUARDS

| Standards | Sections | Implementation Specifications | Required/ Addressable | Description |
|---|---|---|---|---|
| **Security Management Process**: Implement policies and procedures to prevent, detect, contain, and correct security violations. | 164.308(a)(1) | Risk Analysis | Required | Conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information ("Electronic PHI") held by the covered entity |
| | | 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 covered entity. |
| | | 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. |
| **Assigned Security Responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by the Security Rule. | 164.308(a)(2) | | Required | |

| | | | | |
|---|---|---|---|---|
| **Workforce Security:** Implement policies and procedures to ensure that all workforce members have appropriate access to Electronic PHI, as provided under the Information Access Management Safeguards (below), and to prevent those workforce members who do not have access under those standards from obtaining access to Electronic PHI. | 164.308(a)(3) | Authorization and/or Supervision | Addressable | Implement procedures for the authorization and/or supervision of workforce members who work with Electronic PHI or in locations where it might be accessed. |
| | | Workforce Clearance Procedures | Addressable | Implement procedures to determine that the access of a workforce member to Electronic PHI is appropriate. |
| | | Termination Procedures | Addressable | Implement procedures for terminating access to Electronic PHI when the employment of a workforce member ends or as required by determinations made as specified by the workforce clearance procedures. |
| **Information Access Management**: Implement policies and procedures for authorizing access to Electronic PHI. | 164.308(a)(4) | Isolating Health Care Clearinghouse Functions | Required | In the event a covered entity is a health care clearinghouse, if the clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the Electronic PHI of the clearinghouse from unauthorized access by the larger organization. |
| | | Access Authorization | Addressable | Implement policies and procedures for granting access to Electronic PHI, 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 entity's Access Authorization policies (above), establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. |
| **Security Awareness and Training:** Implement a security awareness and training program for all workforce members (including management). | 164.308(a)(5) | Security Reminders | Addressable | Periodic security updates. |
| | | Protection from Malicious Software | Addressable | Address how to implement procedures for guarding against, detecting, and reporting malicious software. |
| | | Log-in Monitoring | Addressable | Address how to implement procedures for monitoring log-in attempts and reporting discrepancies. |
| | | Password Management | Addressable | Address how to implement procedures for creating, changing, and safeguarding passwords. |
| **Security Incident Procedures**: Implement policies and procedures to address security incidents. | 164.308(a)(6) | Response and Reporting | Required | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmless effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. |

| | | | | |
|---|---|---|---|---|
| **Contingency Plan**: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain Electronic PHI. | 164.308(a)(7) | Data Backup Plan | Required | Establish and implement procedures to create and maintain retrievable exact copies of Electronic PHI. |
| | | 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 Electronic PHI while operating in emergency mode. |
| | | Testing and Revision Procedures | 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. |
| **Evaluation**: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security rule and subsequently in response to environmental or operational changes affecting the security of Electronic PHI, that establishes the extent to which an entity's security policies and procedures meet the Security Rule's requirements. | 164.308(a)(8) | | Required | |

| | | | | |
|---|---|---|---|---|
| **Business Associate Contracts and Other Arrangements**: A covered entity may permit a business associate to create, receive, maintain, or transmit Electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory written assurances that the business associate will appropriately safeguard the information. (Section 164.308(b)(2) provides three transmissions to which the standard does not apply, including the transmission of Electronic PHI by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent the plan documents provide that the plan sponsor will reasonably and appropriately safeguard Electronic PHI.) | 164.308(b)(1) | Written Contract or Other Arrangement | Required | Document the satisfactory assurances required through a written contract or other arrangement with the business associate that meets the applicable requirements of Section 164.314(a).<br><br>Note that a covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with this Standard, Implementation Specification, and the business associate agreement requirements. |

## PHYSICAL SAFEGUARDS

| Standards | Sections | Implementation Specifications | Required/ Addressable | Description |
|---|---|---|---|---|
| **Facility Access Controls**: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. | 164.310(a)(1) | 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 (above) and Emergency Mode Operation Plan (above) in the event of an emergency. |
| | | Facility Security Plan | Addressable | Address the implementation of policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft |
| | | Access Control and Validation Procedures | Addressable | Address the implementation of procedures to control and validate a person's access to facilities based on one's role or function, including visitor control, and control of access to software programs for testing and revision. |
| | | Maintenance Records | Addressable | Address the implementation of policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks). |
| **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 Electronic PHI. | 164.310(b) | | Required | |
| **Workstation Security**: Implement physical safeguards for all workstations that access Electronic PHI, to restrict access to authorized users. | 164.310(c) | | Required | |

| | | | | |
|---|---|---|---|---|
| **Device and Media Controls**: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain Electronic PHI into and out of a facility, and the movement of these items within the facility. | 164.310(d)(1) | Disposal | Required | Implement policies and procedures to address the final disposition of Electronic PHI, and/or the hardware or electronic media on which it is stored. |
| | | Media Re-use | Required | Implement procedures for removal of Electronic PHI 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 Electronic PHI, when needed, before movement of equipment. |

## TECHNICAL SAFEGUARDS

| Standards | Sections | Implementation Specifications | Required/ Addressable | Description |
|---|---|---|---|---|
| **Access Control**: Implement technical policies and procedures for electronic information systems that maintain Electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified by the Information Access Management procedures (above). | 164.312(a)(1) | Unique User Identification | Required | Assign an unique name and/or number for identifying and tracking user identity. |
| | | Emergency Access Procedure | Required | Establish (and implement as needed) procedures for obtaining necessary Electronic PHI during an emergency. |
| | | Automatic Logoff | Addressable | Implement electronic procedures that terminate an electronic session after a pre-determined time of inactivity. |
| | | Encryption and Decryption | Addressable | Implement a mechanism to encrypt and decrypt Electronic PHI. |
| **Audit Controls**: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic PHI. | 164.312(b) | | Required | |
| **Integrity**: Implement policies and procedures to protect Electronic PHI from improper alteration or destruction. | 164.312(c)(1) | Mechanism to Authenticate Electronic PHI | Addressable | Implement electronic mechanisms to corroborate that Electronic PHI has not been altered or destroyed in an unauthorized manner. |
| **Person or Entity Authentication**: Implement procedures to verify that a person or entity seeking access to Electronic PHI is the one claimed. | 164.312(d) | | Required | |
| **Transmission Security**: Implement technical security measures to guard against unauthorized access to Electronic PHI that is being transmitted over an electronic communications network. | 164.312(e)(1) | Integrity Controls | Addressable | Implement security measures to ensure that electronically transmitted Electronic PHI is not improperly modified without detection until disposed. |
| | | Encryption | Addressable | Implement a mechanism to encrypt Electronic PHI whenever deemed appropriate. |