Security of Electronic Health Information Under HIPAA
Security of Electronic Health Information Under HIPAA

Course Description

When Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it recognized that, among other things, the confidentiality and integrity of electronic health information must be protected against improper access, disclosure, and manipulation. The HIPAA Security Standards require measures to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) while it's being stored and exchanged. This course will help you understand these standards, what procedures your organization must implement to comply with the law, and what actions to take to secure electronic health information.
# Table of Contents

## Introduction

**Who and What Are Covered**

- Overview .......................................................................................................................... 7
- Privacy and Security Standards .......................................................................................... 10
- Who's Covered? ................................................................................................................... 13
- What Information Is Protected? ......................................................................................... 22
- Bottom Line ....................................................................................................................... 26

## Implementation and Technical Safeguards

- Overview .......................................................................................................................... 27
- Implementation Specifications ......................................................................................... 30
- Safeguards for Access and Audit Control ......................................................................... 37
- Integrity, Authentication, and Transmission Safeguards .................................................. 42
- Bottom Line ....................................................................................................................... 47

## Administrative and Physical Safeguards

- Overview .......................................................................................................................... 48
- Security Management and Responsibility Safeguards ...................................................... 52
- Workforce Security and Access Management ................................................................. 57
- Security Training, Procedures, and Evaluation ................................................................. 61
- Physical Safeguards .......................................................................................................... 67
- Bottom Line ....................................................................................................................... 72

## Knowledge Check

- Top Ten ............................................................................................................................. 76

## FAQ

- Self-Check - Answers ......................................................................................................... 82
Global Insurance is revamping its Website's customer interface. Nancy, from ABC Consulting, is directing the project. Marv, the head of Global's IT department, meets with Nancy to review the site changes in progress.

Marv: Hey Nancy. So you've got some changes to show us?

Nancy: Yes, I can show you the progress we've made. The site is looking really good.

Marv: Great. Sonya here has asked to take a look also. She's Global's new security officer.

Nancy: Oh, good to meet you. So, you'll have a strong eye for the Web site's security issues.
Sonya: Yes, since HIPAA's privacy rules were enacted, the way we secure our customers' information, especially electronically, is crucial. And of course, we'll have to comply with the security standards.

Marv: Yep. Privacy and security have become high priority around here.

Sonya: We'll need to be sure that we're following all the administrative, technical, and physical safeguards for both privacy and security.

Marv: Yep, yep, yep. All those safeguards...

Nancy: Of course, security is a big priority. I have to be honest though. I haven't worked with healthcare material before, so I'll need some guidance.
Marv: Well, most of it is common sense really—isn’t it, Sonya?

Sonya: I suppose you could say that. But we do need to carefully analyze our current system. We need to see what safeguards have been implemented and what other standards we may need to introduce.

Marv: You know, off the record, these HIPAA standards give me a bit of a headache.

Sonya: I’ll keep that off the record, Marv, but I suggest you get used to them. They’re not just industry requirements, they’re the ethical way to serve our customers.
Introduction

Marv and the rest of the company should indeed get used to the standards. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) directed the U.S. Department of Health and Human Services (HHS) to adopt standards that require routine healthcare transactions to be performed electronically.

HIPAA changed the way healthcare professionals handle patient information. Along with privacy comes a healthcare entity’s responsibility for information security. The security obligations may be system wide for large healthcare businesses, or comparatively small for less complicated entities. The security rules are comprehensive but they allow for a large degree of local flexibility in implementation.

Top Ten

The Security Standards require measures to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) while it's being stored and exchanged.

Protection of the privacy of health information depends in part on security safeguards to ensure that data is available when needed and isn't wrongly accessed, altered, or deleted while being stored or transmitted.
Introduction

To protect electronic health information against improper use, HHS developed Privacy Standards and Security Standards.

Click on each image to find out more.

Privacy Standards
The Privacy Standards restrict the use and disclosure of individually identifiable health information (except when this information is contained in certain education and employment records).

Security Standards
The Security Standards require measures to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) while it’s being stored and exchanged.
Introduction

This course will help you understand HIPAA's security standards, what procedures your organization should have in place to comply with the regulations, and what actions to take to secure electronic health information.

This course provides a general overview of the HIPAA Security Standards. It doesn't provide legal advice or technical guidance as to the specific procedures any particular organization should take to protect its electronic protected health information (e-PHI). HIPAA and the security of electronic data are highly technical subjects that can't be completely covered in a brief treatment of this kind. Always consult your internal management, or law and technology departments, about any questions or concerns you have regarding the security measures that these standards require.
Who and What Are Covered

Overview

In this lesson, you will learn

- the relationship between the Security Standards and the Privacy Standards
- which entities are covered by the standards
- what health information is protected
Who and What Are Covered

Overview

Nancy demonstrates the redesigned Website for Marv and Sonya.

Nancy: As you can see, this design really enhances the experience for the user.

Marv: Yeah. Looks good. To tell you the truth, we're more concerned with—and I'm sure Sonya here will agree—what goes on behind the scenes, if you know what I mean.

Nancy: Behind the scenes?

Sonya: I believe Marv is talking about the security issues we mentioned earlier—how we can guarantee the integrity of customer information we receive over the Internet.

Nancy: Gotcha.
Who and What Are Covered

Overview

**Marv:** I mean, in-house, we have all kinds of safeguards—confidentiality agreements and access controls—to limit what information an employee sees.

**Sonya:** We need to make sure customer information is secure through the entire process, even before it gets to us.

**Marv:** Yep. You know, like encrypting the unique identifier fields right off the bat.

**Sonya:** Of course. And we'll help with the other privacy and security standards we need to meet.
Who and What Are Covered

Privacy and Security Standards

Sonya is aware that the Privacy Standards and the Security Standards are interrelated. Protection of the privacy of health information depends in part on security safeguards to ensure the data is available when needed and isn't wrongly accessed, altered, or deleted while being stored or transmitted. The standards also require safeguards on the uses and disclosures of the information even when it is safely stored.

The Security Standards provide a framework for the first set of safeguards; the Privacy Standards address the second set. Those entities that are required to comply with the Privacy Standards must also comply with the Security Standards.

Did You Know?

Later in the course, we'll discuss the various actions an organization covered by HIPAA must take to secure the e PHI it handles.
Who and What Are Covered

Privacy and Security Standards

The Security Standards require a covered entity to implement reasonable and appropriate administrative, physical, and technical safeguards to

- ensure the confidentiality, integrity, and availability of all the e PHI it creates, transmits, receives, or maintains
- protect against reasonably anticipated threats or hazards to its e PHI
- protect against any reasonably anticipated uses or disclosures of e PHI that aren't permitted under the Privacy Standards
- ensure its workforce will comply with its security policies and procedures

PIN: *******
Who and What Are Covered

Privacy and Security Standards

Self-Check

What must the safeguards that a covered entity implements do to meet the Security Standards?

*Check all that apply.*

- Ensure the confidentiality, integrity, and availability of all e-PHI it creates, transmits, receives, or maintains.
- Protect against reasonably anticipated threats or hazards to its e-PHI and against any reasonably anticipated use not allowed by the Privacy Standards.
- Cover both paper and electronic records.
- Ensure its workforce will comply with its security policies and procedures.
Who and What Are Covered

Who's Covered?

The Security Standards apply to the same entities as the Privacy Standards. They also apply to an entity's business associates. The three categories of covered entities are health plans, healthcare clearinghouses, and healthcare providers who transmit PHI electronically in connection with standard transactions. All officers and employees of an organization are required to follow the safeguards, regardless of whether they work on-site or remotely from home or another location.

Let's explore these types of healthcare entities further.
Who and What Are Covered

Who's Covered?

A **health plan** is an organization that provides or pays the cost of medical care. Health plans include health insurance companies, group health plans, and health maintenance organizations (HMOs). The term "health plan" also includes government-administered health benefit programs such as Medicare, Medicaid, Department of Veterans Affairs programs, and TRICARE (Department of Defense).

**Healthcare clearinghouses** are public or private entities that process healthcare transactions. A clearinghouse accepts PHI from one source, converts the information to the standard format, and transmits the information to another entity. The most common type of clearinghouse is a billing company that submits health insurance claims to health plans on a healthcare provider's behalf.
Who and What Are Covered

Who's Covered?

A healthcare provider is a person or other entity that provides, bills for, or is paid for healthcare services in the normal course of business, or one Medicare recognizes as a provider. Hospitals, physicians, skilled nursing facilities, home healthcare agencies, clinical laboratories, medical equipment suppliers, and other licensed/certified healthcare professionals are all considered healthcare providers.

The Security Standards only apply to healthcare providers that transmit PHI electronically in connection with particular transactions identified by Congress. These transactions include healthcare claims and status reports; payment and remittance advice; eligibility determinations for health plan benefits; referral certifications and authorizations; health plan enrollment, disenrollment, coverage eligibility, and premium payments; coordination of benefits; and first reports of injury.
Who and What Are Covered

Who's Covered?

The Security Standards also apply to certain groups made up of covered entities, called affiliated covered entities and organized healthcare arrangements. Entities whose business isn't primarily healthcare related, but that operate as a health plan, healthcare clearinghouse, or a healthcare provider, may be considered hybrid entities. Only the healthcare component of hybrid entities is subject to the Security Standards.

The Security Standards permit affiliated covered entities to designate themselves as a single covered entity for purposes of complying with the rule. Affiliated entities are two or more legally separate healthcare entities under common ownership or common control. These entities can share e-PHI with each other, provided they comply with both the Privacy Standards and the Security Standards.

FAQ

For purposes of affiliated entities, when do common ownership and control exist?

With respect to affiliated entities, common ownership exists if one of the involved organizations owns at least 5% of another organization. Common control means an organization has the power to significantly influence or direct the actions or policies of another organization.
Who and What Are Covered

Who's Covered?

An organized health care arrangement (OHCA) may be formed between legally separate covered entities that integrate their clinical and administrative operations. OHCAs differ from affiliated covered entities in that they aren't necessarily related to each other through common ownership or control.

An example of an OHCA is a healthcare system that includes different types of healthcare providers, like hospitals, medical staff, an ambulatory surgery center, and so on. Each member of the OHCA must comply with the Security Standards.
Who and What Are Covered

Who's Covered?

A person or entity is considered a business associate if it performs services or functions for a covered entity or provides legal, accounting, management, consulting, accreditation, financial, or operational services for the entity that involve using the e-PHI the entity holds. Employees, volunteers, trainees, and other persons working under the direct control of the covered entity are not business associates.
Who and What Are Covered

Who's Covered?

Under the Security Standard dealing with business associate contracts and other arrangements, a covered entity may let a business associate create, receive, maintain, or transmit e-PHI on its behalf. However, with some exceptions, the covered entity and its business associate must first enter into a contract requiring the business associate to

- implement administrative, physical, and technical safeguards to protect the e-PHI
- make sure any agent or subcontractor the associate provides the e-PHI to agrees to implement safeguards to protect it
- report any security incidents to the entity
- make its policies available to the HHS to determine compliance with the standards

The contract must also allow the entity to terminate it if the business associate violates the agreement.

Under a recent law, business associates will be directly subject to the Security Standards starting in early 2010. However, business associate contracts are still required.

Did You Know?

To comply with the Privacy Standards, the contract must, among other things, establish how the associate will use and disclose the e-PHI.
Who and What Are Covered

Who's Covered?

Generally, a covered entity isn't expected to monitor its business associates, but when an organization learns of potential violations, it must investigate. An organization is only responsible for security violations committed by a business associate if the organization knows of the wrongdoing and fails to take steps to stop it and limit any harm.

If an organization can't, with reasonable effort, correct the business associate's Security Standard violation, it must terminate the business associate contract or report the violation to the U.S. Department of Health and Human Services.

FAQ

What if terminating a contract with a business associate poses a hardship for the organization?

If terminating the relationship due to a violation isn't possible or would cause significant hardship for the covered organization, it must report the situation to HHS.
Who and What Are Covered

Who's Covered?

Self-Check

Davis Eye Care, a large ophthalmology group practice, submits claims for its services electronically. Once a year, it hires a coding and billing consultant to audit its claims to ensure the practice is billing for its services accurately. In order to perform the audit, the consultant requires the clinical and billing records for a sample of services furnished by the practice to patients. The practice provides the patient information to the consultant electronically.

Is the consultant considered a business associate under Privacy and Security Standards?

☐ Yes
☐ No
Who and What Are Covered

What Information Is Protected?

PHI is defined as individually identifiable health information (IIHI) (not contained in certain education and employment records) that is transmitted or maintained by a covered entity or business associate.

For purposes of the Privacy Standards, PHI is IIHI maintained in any format (electronic, oral, or paper). The Security Standards, however, pertain only to e-PHI. E-PHI includes information maintained or transmitted in any type of electronic media, but doesn't include paper information transmitted by facsimile.
Who and What Are Covered

What Information Is Protected?

IIHI is a broader category, including any health, financial, and demographic information that is created or received by a covered entity, identifies the individual who is the subject of the information, and relates to one of the following:

- An individual's past, present, or future physical or mental health or condition
- An individual's healthcare
- An individual's provision for past, present, or future payment for healthcare
Who and What Are Covered

What Information Is Protected?

Covered entities and business associates can de-identify PHI by removing all information that identifies an individual or that could likely be used to identify an individual. Properly de-identified PHI is not subject to the Security Standards because it's no longer considered protected information.

There are two ways to de-identify health information. The first involves removing all identifying characteristics, such as names and addresses, social security numbers, identifiable photographs, and medical record numbers, along with other information.

A covered entity can also determine that PHI is not individually identifiable if a qualified statistician examines the information and determines that the risk of reidentification is very small.

FAQ

What unique identifiers must be removed to de-identify health information?

To de-identify PHI, a covered entity or business associate must remove all identifying characteristics, including such information as names and addresses, dates, social security numbers, medical record numbers, telephone and fax numbers, e-mail and other Internet addresses, health insurance numbers, and identifiable photographs. Other identifiers may include account numbers, vehicle identifiers, and driver's license numbers. Information relating to gender, race, ethnicity, and marital status isn't individually identifiable and doesn't have to be removed.
Dr. Martin is an internist in Albany, New York. One of his patients, Steve, gets sick while visiting New York City and has some laboratory tests done while he's there. The lab then faxes the results to Dr. Martin.

Which of the following statements is true in this situation?

- The Security Standards apply because the lab tests are PHI.
- The Security Standards apply because the lab results identify Steve and discuss his condition.
- The Security Standards don't apply because the lab tests were faxed to Dr. Martin.
- The Security Standards don't apply because Steve is Dr. Martin's patient.
Who and What Are Covered

Bottom Line

HIPAA's Privacy and Security Standards are closely linked. Protecting the privacy of health information requires implementing security safeguards to ensure the data is available when needed, and it's not wrongly accessed. So, your organization must follow the standards for privacy as well as for security.

The standards cover healthcare entities including health plans and healthcare clearinghouses, and healthcare providers who transmit PHI electronically in connection with standard transactions. They also apply to an entity's business associates.

Protected health information that's covered under the Security Standards includes any individually identifiable health information (not contained in certain education and employment records) that's transmitted or maintained in electronic format.
Implementation and Technical Safeguards

Overview

In this lesson, you will learn about

- implementation and documentation requirements under the Security Standards
- safeguards for controlling the access to and auditing of information
- safeguards for information integrity, authentication, and transmission
Overview

**Sonya:** Hi Marv. How's everything going in IT?

**Marv:** Fine, just making sure we're ready for the new site. What's up?

**Sonya:** Now that our system is secure for purposes of the Privacy Rules, we need to make sure our security measures meet the Security Standards, too.

**Marv:** I've been looking at those. I think we're in good shape.

**Sonya:** How so?

**Marv:** Well, for one thing, we have some access controls in place for all the employees here.

**Sonya:** I've noticed, though, that they seem to depend on which department you're in.
Implementation and Technical Safeguards

Overview

**Marv:** Uh-huh. Access is granted based on job description. Just like you said it's explained in the standards.

**Sonya:** That's well and good, but it seems that if I go down to the billing department, I can sit down at any computer and pull up Joe Client's billing records…

**Marv:** Well those employees need that access.

**Sonya:** …and health records.

**Marv:** Oh. Well we've been meaning to implement an automatic logoff when the computer isn't in use.

**Sonya:** We don't have that set up yet?

**Marv:** Uh, well…no.
Implementation and Technical Safeguards

Implementation Specifications

It looks like Marv and his IT department better start addressing some of these security issues. A covered entity is expected to assess its own security risks and implement appropriate measures to address its security needs. For the most part, covered entities can use the security measures of their choice to reasonably and appropriately address their own unique circumstances.

If a healthcare organization like Global has poor or nonexistent access controls on its databases, it will be more susceptible to hacking than an organization with protections in place, and will have to work harder to comply with the Security Standards. If an organization is already following a security plan, it need only make certain that the plan is actually being followed and continues to be effective.

Top Ten

The Security Standards require covered entities to implement reasonable and appropriate administrative, physical, and technical safeguards.

These safeguards seek to ensure the confidentiality, integrity, and availability of all the e-PHI they create, transmit, receive, or maintain; protect against reasonably anticipated threats or hazards to the security or integrity of their e-PHI; protect against uses or disclosures of the e-PHI that aren't required or permitted under the Privacy Standards; and ensure their workforce will comply with their security policies and procedures.
Implementation and Technical Safeguards

Implementation Specifications

Covered entities may decide how to satisfy the security requirements and which technologies to use. In doing so, they must consider:

- their size, complexity, and capabilities
- their technical infrastructure, hardware, and software security capabilities
- the cost of security measures
- the probability and degree of potential risks to e-PHI they store or transmit
Implementation and Technical Safeguards

Implementation Specifications

While the Security Standards allow for a lot of flexibility, many of them provide instructions in the form of implementation specifications.

Implementation specifications are either required or addressable. A covered entity must implement required specifications as part of its security programs.

On the other hand, if a specification is addressable, an organization must assess whether it’s reasonable and appropriate to adopt the specification, based on the level of security risk, the effectiveness of other security measures in place, and the cost involved. If the organization determines that the measure is reasonable, it must use it.

Did You Know?

Some standards don’t contain a corresponding implementation specification because the standards themselves give enough instruction to guide implementation.
Implementation and Technical Safeguards

Implementation Specifications

If a covered entity decides that it's not appropriate to implement an addressable specification, it can opt not to, as long as it documents how and why it reached this conclusion.

It's important to keep in mind that the organization is responsible for meeting each of the HIPAA standards for administrative, physical, and technical safeguards and must maintain a written record of how this is accomplished. Also, if a covered entity decides not to follow an addressable implementation specification, it must adopt an equivalent security measure.
Implementation and Technical Safeguards

Implementation Specifications

Besides complying with the standards that address the various vulnerabilities of electronic information systems, the Security Standards also impose certain documentation requirements:

- Every entity must implement appropriate measures to comply with the safeguards.
- Policies and procedures must be retained for six years from the later of the date of creation or when last in effect.
- The policies and procedures must be made available to those responsible for implementing the procedures described in the documentation.
- An entity must review its documentation periodically in response to changes in its security environment and business operations.

The policies and procedures, and any challenges to them, must be in writing and maintained.
Implementation and Technical Safeguards

Implementation Specifications

An organization has to decide what information employees can have access to, and then verify that its procedures comply with federal regulations. Although software tools can be helpful in this process, complete automation may not yet be available in all cases.
Implementation and Technical Safeguards

Implementation Specifications

Self-Check

Dr. Sanchez is a sole practitioner and a covered entity. She employs two people, as her medical technicians and to handle office administration. The workforce security standard has an addressable implementation specification (called workforce clearance procedure) suggesting that she limit her employees’ e-PHI access to what their jobs require. Nevertheless, she decides—and documents the reason for her decision—not to grant varying levels of access to e-PHI, because both employees require equal access. However, Dr. Sanchez’s practice is growing.

What should she do when she hires a new employee?

☐ Continue with the same practices without making policy changes.
☐ Review her decision regarding the addressable specification.
☐ Stop accepting patients now to keep the practice small.
☐ Hire a clearinghouse to handle the e-PHI.
Implementation and Technical Safeguards

Safeguards for Access and Audit Control

A covered entity must implement technical safeguards as part of its security plan to protect the e-PHI it handles. These safeguards refer to the use of certain types of available technology to protect e-PHI by controlling access to it. There are five standards an organization must address. Several of the standards contain implementation specifications that are addressable, while the access control standard contains both addressable and required specifications.

Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on HIPAA's information access management standard under the administrative safeguards. We'll talk more about these safeguards in the next lesson.
Safeguards for Access and Audit Control

In addition to regulating access to e-PHI under normal conditions, procedures must be in place to let people access needed e-PHI during an emergency. Depending on the type of emergency, programmed access controls may not be operable, and access could be denied to even those cleared for access. Guidance should be developed beforehand to help credentialed users gain access to critical systems during emergency conditions.

While the two implementation specifications referenced above are required, the access control standard also has two addressable specifications. Covered entities need to decide whether to implement an automatic logoff to terminate an electronic session after a set length of time, and whether to use encryption as a method to deny access to the e-PHI they store and transmit.
Implementation and Technical Safeguards

Safeguards for Access and Audit Control

HIPAA's security breach notification requirement, added in 2009, offers guidance on the use of encryption. The rule requires a HIPAA covered entity to provide notification to individuals when there is a breach of unsecured personal health information that compromises the security or privacy of the information.

However, the rule only applies to a breach of unsecured protected health information. PHI is unsecured if it is not rendered unusable, unreadable, or indecipherable to unauthorized individuals using a technology or methodology specified by the HHS.

Thus, if e-PHI is encrypted to the HHS standard, a security breach notification is not required. A covered entity may find this benefit relevant in making decisions about whether and how to encrypt e-PHI.
Implementation and Technical Safeguards

Safeguards for Access and Audit Control

The audit controls standard requires that covered entities implement hardware, software, or procedural mechanisms that monitor PHI activity in information systems. Audit controls might track the identity of a user, the description of the e-PHI accessed, the site of the request, and the reason for accessing the e-PHI.

By reviewing audit results, a covered entity can monitor potentially inappropriate or unusual access patterns of a user or certain e-PHI.

The standards don’t dictate the type of audit control system to be used. The system should be based on a covered entity’s risk assessment or risk analysis.

Top Ten

Organizations must consider several factors when adopting security measures.

How a covered entity satisfies the security requirements and which technology it decides to use are business decisions left to the individual organization. In deciding what security measures to adopt, an organization must consider its size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; the cost of particular security measures; and the probability and degree of the potential risks to the e-PHI it stores and transmits.
Implementation and Technical Safeguards

Safeguards for Access and Audit Control

Self-Check

The access controls standard requires users to be assigned unique names or numbers for access control and tracking purposes.

☐ True
☐ False
Implementation and Technical Safeguards

Integrity, Authentication, and Transmission Safeguards

The additional technical safeguards an entity must implement are the standards for integrity, authentication, and transmission. The integrity standard requires covered entities to protect e-PHI from improper alteration or destruction.

The goal of this standard is to assure organizations that the data they use to make decisions and release to others hasn’t been altered inappropriately. Organizations should consider whether to implement electronic mechanisms to verify that the e-PHI has remained under their control.

FAQ

What tools can be used to ensure the integrity of electronic information?

Depending on an organization's identified level of security risk, it may use electronic mechanisms such as error-correcting memory, magnetic disk storage systems, digital signatures, or check-sum technology. These will help authenticate that e-PHI has not been altered or destroyed in an unauthorized manner.
Implementation and Technical Safeguards

Integrity, Authentication, and Transmission Safeguards

Under the **authentication** standard, organizations must implement systems to verify the identity of users attempting to access e-PHI. Authentication mechanisms include unique user IDs, which are required under the access control standard discussed earlier.

Other potential systems include biometric identification systems, passwords, personal identification numbers, and telephone call-back or token systems.
Implementation and Technical Safeguards

Integrity, Authentication, and Transmission Safeguards

The last standard under the technical safeguards focuses on securing e-PHI during its transmission over a communication network. There are no required implementation specifications. However, covered entities are expected to consider the addressable issues of whether to use encryption and whether to prevent e-PHI from being wrongly modified until it's disposed of.

Did You Know?

As with all addressable specifications, your organization must decide, based on its individual level of risk, whether it's appropriate to implement any kind of transmission mechanism into its overall security plan.
Implementation and Technical Safeguards

Integrity, Authentication, and Transmission Safeguards

Some of the standards covered under this rule may already be required under the technical safeguards of the Privacy Standards. All covered entities should assess their security risks and current infrastructure to protect e-PHI.

Security guidance documents are available on the OCR Web site.
Implementation and Technical Safeguards

Integrity, Authentication, and Transmission Safeguards

Self-Check

According to the technical safeguards, which of the following is true?

Check all that apply.

☐ The authentication standard requires unique user IDs.

☐ The transmission standard has two required implementation specifications.

☐ Organizations should consider addressable transmission issues and implementing measures to prevent e-PHI from being modified improperly.

☐ The goal of the integrity standards is to assure organizations that the data they make decisions on is intact.
Implementation and Technical Safeguards

Bottom Line

Your organization is expected to assess its own security risks and implement appropriate measures to address its security needs. For the most part, it can use the security measures of its choice to reasonably and appropriately address its own unique circumstances.

However, a covered entity must implement certain technical safeguards as part of its security plan to protect the e PHI it handles by controlling access to it. There are five standards an organization must address, one of which, access control, has required and addressable implementation specifications, and a few of which have only addressable specifications. All covered entities are encouraged strongly to assess their security risks and current infrastructure. Significant risks to patient or enrollee privacy should be addressed now.
Administrative and Physical Safeguards

Overview

In this lesson, you will learn about the

- administrative standards for security management and responsibility
- administrative standards for workforce security and information access management
- administrative standards for security awareness training, incident procedures, contingency plans, and evaluations
- physical safeguards for securing equipment and physical property
Administrative and Physical Safeguards

Overview

Sonya and Marv are talking on the phone in the midst of a thunderstorm.

Sonya: Hi Marv. Wow, what a storm outside! Just wanted to touch base on how the risk analysis is going for the IT department.

Marv: Oh, yes, we've made a lot of progress.

Sonya: Are the automatic logoffs in place?

Marv: They are. I think we really have things secure now.
Overview

Sonya: Good. Wow, look at that lightning! Are we set up to handle a brownout or a blackout?

Marv: We've never had one, but we're definitely ready.

Sonya: We can still access the records we need if the electricity goes out?

Marv: You bet your boots we can.
Administrative and Physical Safeguards

Overview

*Half an hour later, the electricity goes out at Global Insurance.*

**Sonya:** You're saying the system is down?

**Marv:** It's the darnedest thing…

**Sonya:** This isn't good, Marv, this really isn't good.

**Marv:** Well, at least the phones are still working and… Hello? Hello?
Administrative and Physical Safeguards

Security Management and Responsibility Safeguards

Looks like Global Insurance is learning the hard way about the emergency safeguards it should have put in place. HIPAA’s administrative safeguards require covered entities to develop and implement a security management process that includes policies and procedures to address the full range of potential security vulnerabilities, including power outages.

Let's take a look at the standards an organization has to implement to comply with these safeguards.
Administrative and Physical Safeguards

Security Management and Responsibility Safeguards

Covered entities must design policies and procedures to prevent, detect, contain, and correct security violations. To meet the security management process standard, an organization has to implement four required specifications into its security plan: risk analysis, risk management, sanction policy, and periodic reviews.

FAQ

What general requirements of the Security Standards does an organization have to meet?

The general requirements of the Security Standards are to ensure the confidentiality, integrity, and availability of all e-PHI it creates, receives, maintains, or transmits; protect against reasonably anticipated threats or hazards to the security or integrity of its e-PHI; protect against any reasonably anticipated uses or disclosures of the e-PHI that aren't required or permitted under the Privacy Standards; and ensure its workforce complies with its security policies and procedures.
Administrative and Physical Safeguards

Security Management and Responsibility Safeguards

Click on each image to find out more about the security management process requirements.

Risk analysis
A thorough risk analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI.

Risk management
A risk management process to identify and implement appropriate security measures based on the risk analysis and the entity's specific circumstances. The security measures must be sufficient to reduce the risks and vulnerabilities to an appropriate level and allow the entity to comply with the general requirements of the Security Standards.

Sanction policy
A sanction policy applicable to employees who fail to comply with the security measures.
Administrative and Physical Safeguards

Periodic reviews
Periodic reviews of information system activity, such as audit logs, access reports, and security incident tracking reports.
Administrative and Physical Safeguards

Security Management and Responsibility Safeguards

The assigned security responsibility standard requires an organization to designate someone as its security officer. This person is in charge of developing and implementing the measures determined by the organization to be necessary for it to protect the e-PHI it stores and transmits. This standard doesn't contain any implementation specifications.
Administrative and Physical Safeguards

Workforce Security and Access Management

As part of the workforce security standard, covered entities must implement measures to determine and assign user access privileges. To do so, a covered entity must decide what programs and what particular data within those programs an employee needs to access.

Access restrictions should depend on an employee's job description and the type of e-PHI he or she needs to do a job. Access privileges also may be designed to control her ability to read, write, or amend e-PHI. These policies also must tell how an organization plans to prevent employees from getting access to e-PHI they're not allowed to access.

FAQ

What are the documentation specifications of the Security Standards?

Along with requiring compliance to address the vulnerabilities of electronic information systems, the Security Standards also impose documentation requirements. That is, every covered organization must implement policies and procedures to comply with HIPAA's safeguards; these policies must be retained for six years; they must be made available to those responsible for implementing the procedures described in the documentation; and an organization must review its documentation periodically in response to changes in its security environment and business operations.
Administrative and Physical Safeguards

Workforce Security and Access Management

The workforce security standard has no required specifications and three that are addressable: authorization and supervision, workforce clearance procedures, and termination procedures.

The authorization and supervision specification instructs covered entities to determine whether it's necessary, for purposes of protecting PHI, to supervise employees who work with e-PHI or the locations where e-PHI might be accessed. Workforce clearance procedures direct covered entities to consider whether they need formal procedures to determine if employees have the right access privileges. Termination procedures describe how a covered entity will end employees' ability to access e-PHI once they are no longer with the company.
Administrative and Physical Safeguards

Workforce Security and Access Management

Under the information access management standard, an organization must have policies and procedures to authorize access to e-PHI consistent with the Privacy Standards.

This standard also includes two addressable specifications. Under the first, an organization should, as appropriate, determine whether to implement measures to grant employees access to its e-PHI based on workstation, type of transaction, program, or process. The second specification tells the organization to decide whether it should formally evaluate a user's level of access and modify it as needed.

Did You Know?

When a healthcare clearinghouse is part of a larger organization, the clearinghouse is required to have measures to protect its e-PHI from unauthorized access by the larger organization.
New Point Ambulatory Surgery Center employs 25 people in various roles. Some of the employees are clinical staff, such as the operating room nurses, and others perform only administrative duties. New Point has a policy that only members of its billing office may process patient accounts. Nevertheless, the New Point security officer discovers, during his security risk analysis, that some employees who are not billing staff have accessed patient financial records to determine patients' copayment or deductible obligations.

Will the security officer find that the center is in compliance with HIPAA's Privacy and Security Standards?

☐ Probably

☐ Probably not
Administrative and Physical Safeguards

Security Training, Procedures, and Evaluation

All staff members of a covered entity, including management, must participate in security awareness training under the security awareness training standard. The content of this training may be tailored to an employee's functions. At a minimum, however, an organization has to consider whether its training materials should include information relating to four implementation specification topics, all of which are addressable:

- Security reminders
- Procedures for guarding against, detecting, and reporting malicious software
- Procedures for monitoring login attempts and reporting login discrepancies
- Procedures for creating, changing, and safeguarding passwords

Did You Know?

According to CMS, the entity "should" provide periodic retraining "whenever environmental or operational changes affect the security of e-PHI."
Administrative and Physical Safeguards

Security Training, Procedures, and Evaluation

Every covered entity must have policies and procedures to identify, document, and respond to suspected or known security incidents; limit the harmful effects of a known security incident; and document the outcome of the incident. The security incident procedures standard dictates that the policies should identify what types of actions would be considered security incidents, the specific process for documenting incidents, and what information should be contained in an incident report.

Did You Know?

The best response to security incidents depends on your organization's environment and the type of e-PHI involved.
From the Headlines

The HIPAA requirements for Security Standards have been in place since 2005. However, continuing press attention to threats to privacy as a result of inadequate security resulted in further congressional action. In 2009, Congress enacted a separate security breach notification law that applies to HIPAA covered entities.

Notification of breaches can be expensive and highly damaging to an organization's reputation. The best way to avoid these consequences is with a carefully implemented security plan.
Administrative and Physical Safeguards

Security Training, Procedures, and Evaluation

The contingency plan standard allows a covered entity to protect the security of its data during an unexpected event such as a natural disaster. This standard requires organizations to establish procedures for responding to an event such as a fire, an act of vandalism, a system failure, or a natural disaster that damages their systems containing e-PHI.

Minimally, the organization must create and maintain retrievable exact copies of e-PHI, have a recovery plan to restore lost data, and have an emergency operation plan to continue critical business activities to protect the security of the e-PHI while operating in emergency mode.

In addition, the contingency plan may include a schedule for testing and revising it periodically. An organization also may opt to consider which system functions are most critical, and, therefore, most essential to keep operational during an emergency.

Top Ten

The security awareness training standard requires all employees to participate in training.

All staff members of a covered entity, including management, must participate in security awareness training under this standard. This training's content may be tailored to an employee's functions. At a minimum, however, an organization must consider whether its training materials should include information relating to four implementation specification topics, all of which are addressable: security reminders, procedures for guarding against malicious software, procedures for monitoring login attempts and reporting login discrepancies, and procedures for creating, changing, and safeguarding passwords.
Administrative and Physical Safeguards

Security Training, Procedures, and Evaluation

The evaluation standard requires an organization to evaluate its security safeguards periodically to demonstrate and document compliance with its security policies and with the Security Standards.

The evaluations should be performed regularly, as well as when an organization's security environment has changed. For example, a nonroutine evaluation might be warranted to assess the value of a new technology in eliminating or reducing a security risk, or to determine the success of a response to a new security risk.

FAQ

Must the evaluation of an organization's security safeguards be conducted by an external entity?

The evaluation doesn't have to be conducted by an external entity. Staff trained to critique both the technical and nontechnical components of the organization's security plan can perform the evaluation.
ABC Clearinghouse takes pride in its security policies and its well-trained staff. To help ensure that its staff is properly trained in security measures, which of the following could this clearinghouse include in every staff member's training materials?

Check all that apply.

- Security reminders
- Procedures for guarding against malicious software
- Procedures for reporting login discrepancies
- Procedures for safeguarding passwords
The last topic in this course is **physical safeguards**. These are security measures taken to protect an organization's electronic information systems, related equipment, and the buildings housing the systems from natural and environmental hazards, and unauthorized intrusion. There are four standards to be fulfilled. However, because most of the implementation specifications in this category are addressable, organizations have considerable flexibility in how to comply with the requirements.

Let's investigate the physical safeguards now.
Administrative and Physical Safeguards

Physical Safeguards

The facility access control standard focuses on measures to limit physical access to electronic information systems and to the facilities where the systems are housed. The Security Standards don't require any particular measures under this standard, but there are four addressable issues to consider.

First, an organization may design a contingency plan that sets out how to access a facility during disaster recovery or in emergency mode. Next, a facility security plan to shield any buildings housing electronic systems from unauthorized physical access should be considered. Third, an organization should consider whether controlling the access to facilities or systems according to an employee's job functions would decrease security risks. Lastly, an organization may decide to document any modifications related to security made to the facility building.

FAQ

What if the covered organization isn't the only occupant in a building?

A facility security plan should take situations into account where a covered organization isn't the sole occupant of a building. When appropriate, an organization's security plan may include measures that would be taken by a third party or other occupant of a building to protect the physical security of the building.
Administrative and Physical Safeguards

Physical Safeguards

The workstation use standard refers to the functions and physical attributes of a specific workstation, or group of workstations, for maximizing the security of the e-PHI stored in the networks that the workstations access. The standard applies to employees who work from home, in satellite offices, or in another facility.

Under the standard for workstation security, an organization is required to implement physical safeguards to deter unauthorized access. A physical security measure might include locking the door to the part of the facility where the workstation is located or locking the screen of the workstation.
Administrative and Physical Safeguards

Physical Safeguards

Because e-PHI may move through an organization in many forms (via disk or magnetic tape, or as part of a computer network), the device and media controls standard requires that an entity implement measures for controlling the removal of any electronic media that contains e-PHI, either inside or outside of the facility. These policies also must address the final disposition of e-PHI and the hardware or electronic media it's stored on.

The Security Standards allow an organization to decide whether to track the movement of its hardware or software, or who is moving the items, unless there is some other reason already for such documentation. Likewise, the standards permit an organization to decide when it should make an exact copy of e-PHI before moving the equipment that stores or transmits it.

Did You Know?

An organization's policies must have a provision that instructs employees on how to remove e-PHI from electronic media before the media are made public.
Administrative and Physical Safeguards

Physical Safeguards
Self-Check

Fern Landing, a skilled nursing facility, has workstations positioned throughout the facility. Some of the workstations are located in offices, but most are found on the nursing units and are accessible to all residents and their visitors.

What can Fern Landing do to protect the e PHI it handles?

☐ Require photo identification from all visitors to the center.
☐ Require residents to sign a confidentiality agreement.
☐ Create an automatic logoff for all computers.
☐ Discontinue all visiting hours.
Administrative and Physical Safeguards

Bottom Line

HIPAA's administrative safeguards require your organization to implement specific standards for the full range of potential security vulnerabilities. These standards include the security management process, assigned security responsibility, workforce security, information access management, security awareness training, security incident procedures, contingency plan, evaluation, and business associate contracts and other arrangements.

The physical safeguards are security measures designed to protect your organization's electronic information systems, equipment, and facilities from natural and environmental hazards, and unauthorized intrusion. The required standards cover facility access control, workstation use, workstation security, and device and media controls.
Knowledge Check

Questions

1. Which of the following is true regarding a healthcare company complying with the Security Standards?
   - The company has to disclose healthcare information when the media requests it in writing.
   - The company doesn't have to train its workforce in security procedures.
   - The only data that's actually protected in e-PHI are the patient names.
   - The company has to protect its e-PHI against all reasonable threats.

2. A doctor contracts with an accounting firm to handle her patient e-PHI billing. Which of the following statements is true regarding her relationship with her accounting business associate?
   - She must closely monitor the accounting firm's compliance with the Security Standards.
   - She can allow the business associate to transmit e-PHI on her behalf without restriction.
   - The accounting firm must provide written documentation of its proper safeguards to protect the e-PHI she provides.
   - She isn't responsible for investigating concerns she has about the accounting firm's security measures.

3. Dr. Sanchez is participating in a research study and needs to de-identify his patients' records before sending them to the research team. Which of the following methods could he use to properly de-identify the patients' information so it's not subject to the Security Standards?
   - Have his nurse review the records to determine if the risk of reidentification is low.
   - Remove all individually identifiable information.
   - Encrypt the patient's name only.
   - Use only patient photographs to identify the records.

4. A healthcare company develops a plan to put into effect an addressable implementation specification, but determines that it's cost prohibitive. Does the company have to implement the addressable security standard?
   - No, as long as it documents its decision in writing and implements an equivalent measure.
   - No, addressable implementation specifications are completely optional and may be skipped with no further action required.
   - Yes, all implementation specifications must be implemented.
   - Yes, cost is irrelevant.
Knowledge Check

Questions

5. Which of the following is a documentation requirement imposed by the Security Standards?
   - A healthcare provider must review its documentation daily.
   - Policy documentation must be retained for 20 years or the life of the organization.
   - Security procedures developed by health insurance companies must be made available to every employee, whether or not they are subject to them.
   - Every covered healthcare organization must implement appropriate measures to comply with HIPAA’s safeguards.

6. One of the required specifications of the access control standard is to
   - use voice and eye recognition software.
   - use encryption software.
   - assign unique names or numbers to system users.
   - implement automatic logoff for computers.

7. One of the Security Standards’ goals is to protect e-PHI data from being altered or destroyed in an unauthorized way. Which of the following standards covers this goal?
   - Access controls
   - Integrity
   - Authentication
   - Transmission

8. Which of the following must a company implement to meet the security management process standard?
   - Surveillance cameras to monitor computer access
   - Risk analysis to identify potential vulnerabilities
   - Monitoring systems to track login attempts and discrepancies
   - A strict dismissal policy for employees who fail to comply with any security measure
Knowledge Check

Questions

9. A healthcare provider is developing procedures to protect its e-PHI in case of a natural disaster. Which standard covers this type of security?

☐ Evaluation standard
☐ Security awareness standard
☐ Security incident procedures standard
☐ Contingency plan standard

10. Which of the following standards deals with the removal of any electronic media that contains e-PHI?

☐ Facility access control standard
☐ Device and media controls standard
☐ Workstation security standard
☐ Ergonomic comfort standard
• The Security Standards require measures to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI) while it's being stored and exchanged.

Protection of the privacy of health information depends in part on security safeguards to ensure that data is available when needed and isn't wrongly accessed, altered, or deleted while being stored or transmitted.

• The Privacy Standards and the Security Standards are necessarily linked.

Any health record system requires safeguards to ensure the data is available when needed and that information is not used, disclosed, accessed, altered, or deleted inappropriately while being stored or transmitted. The Security Standards work together with the Privacy Standards to establish appropriate controls and protections. Health sector entities that are required to comply with the Privacy Standards also must comply with the Security Standards.

• The Security Standards require covered entities to implement reasonable and appropriate administrative, physical, and technical safeguards.

These safeguards seek to ensure the confidentiality, integrity, and availability of all the e-PHI they create, transmit, receive, or maintain; protect against reasonably anticipated threats or hazards to the security or integrity of their e-PHI; protect against uses or disclosures of the e-PHI that aren't required or permitted under the Privacy Standards; and ensure their workforce will comply with their security policies and procedures.

• The Privacy Standards apply to all protected healthcare information, whereas the Security Standards apply only to e-PHI.

The Privacy Standards apply to protected health information (PHI) in any format. PHI is individually identifiable health information (IIHI) (other than IIHI contained in certain education and employment records). The Security Standards, however, pertain only to electronic PHI (e-PHI). E-PHI is PHI maintained or transmitted in any type of electronic media, but doesn't include paper information transmitted by facsimile. Thus, the scope of PHI that the Security Standards must protect is more limited than that protected by the Privacy Standards.

• Organizations must consider several factors when adopting security measures.

How a covered entity satisfies the security requirements and which technology it decides to use are business decisions left to the individual organization. In deciding what security measures to adopt, an organization must consider its size, complexity, and capabilities; its technical infrastructure, hardware, and software security capabilities; the cost of particular security measures; and the probability and degree of the potential risks to the e-PHI it stores and transmits.

• HIPAA imposes five technical safeguards.

For a covered organization to protect the e-PHI it handles, it must implement technical safeguards as part of its security plan. Technical safeguards refer to using technology to protect e-PHI by controlling access to it. Covered organizations must address five standards focusing on access and audit control, and integrity, authentication, and transmission of e-PHI.

• The integrity standard requires covered organizations to protect e-PHI from improper alteration or destruction.

Data or information that has integrity hasn't been altered or destroyed in an unauthorized manner. Organizations should consider whether to implement electronic mechanisms to check if the e-PHI has remained under their control. The goal of this standard is to assure organizations that the data they use to make decisions and release to others hasn't been so altered or destroyed.
• **HIPAA requires eight different administrative safeguards.**
  These standards include the security management process standard, to prevent security violations; assigned security responsibility, to identify a security officer; workforce security, to determine e-PHI user access privileges; information access management, to authorize access to e-PHI; security awareness training, to train staff members in security awareness; security incident procedures, to handle security incidents; contingency plan, to protect e-PHI during an unexpected event; and evaluation, to evaluate an organization's security safeguards.

• **The security awareness training standard requires all employees to participate in training.**
  All staff members of a covered entity, including management, must participate in security awareness training under this standard. This training's content may be tailored to an employee's functions. At a minimum, however, an organization must consider whether its training materials should include information relating to four implementation specification topics, all of which are addressable: security reminders, procedures for guarding against malicious software, procedures for monitoring login attempts and reporting login discrepancies, and procedures for creating, changing, and safeguarding passwords.

• **Four physical safeguards are required by HIPAA.**
  The required physical standards are the facility access control standard, to limit actual physical access to electronic information systems and the facilities where they're located; the workstation use standard, to control the physical attributes of a specific workstation or group of workstations, to maximize security; the workstation security standard, to implement physical safeguards to deter the unauthorized access of a workstation; and the device and media controls standard, to control the movement of any electronic media containing e-PHI from or within the facility.
Q. Are the Security Standards interrelated with the Privacy Standards?
A. Yes. Any health record system requires safeguards to ensure the data is available when needed and that information is not used, disclosed, accessed, altered, or deleted inappropriately while being stored or transmitted. The Security Standards work together with the Privacy Standards to establish appropriate controls and protections. Health sector entities that are required to comply with the Privacy Standards also must comply with the Security Standards.

Q. Are there any types of insurance organizations to which the Security Standards don't apply?
A. Yes. Workers' compensation, automobile, life, property, and casualty insurers aren't considered to be health plans, and, therefore, need not follow the Security Standards, even if a policy they issue contains coverage of certain healthcare costs.

Q. What is considered a health plan under HIPAA?
A. A health plan is an organization that provides or pays the cost of medical care. Health plans include health insurance companies, group health plans, and health maintenance organizations (HMOs). The term "health plan" also includes government-administered health benefit programs such as Medicare, Medicaid, Department of Veterans Affairs programs, and TRICARE (Department of Defense).

Q. What is a healthcare provider?
A. A healthcare provider is a person or organization that provides, bills for, or is paid for healthcare services in the normal course of business, or one who is recognized by Medicare as a provider. Hospitals, physicians, skilled nursing facilities, home healthcare agencies, clinical laboratories, medical equipment suppliers, and other licensed/certified healthcare professionals are all considered healthcare providers. The Security Standards only apply to healthcare providers that transmit PHI electronically in connection with particular transactions identified by Congress.

Q. What does a typical healthcare clearinghouse do?
A. Healthcare clearinghouses are public or private entities that process or facilitate the processing of healthcare transactions. The clearinghouse accepts PHI from one source, converts the information to the standard format, and transmits it to another organization. The most common type of clearinghouse is a billing company that submits health insurance claims to health plans on behalf of healthcare providers. The healthcare provider sends financial and clinical information to the billing company, and the company formats it into the standard health claims format and then submits the file to a payer.

Q. Which types of transactions must meet the Security Standards?
A. Healthcare providers must comply with the Security Standards if they transmit e-PHI in connection with specific transactions, including healthcare claims and status reports, payment and remittance advice, eligibility determination for health plan benefits, referral certifications and authorization, health plan enrollment, disenrollment, health plan coverage eligibility, premium payments, coordination of benefits, and first reports of injury. If a healthcare provider doesn't perform any of these electronic transactions, it's not required to comply with the Security Standards.

Q. For purposes of affiliated entities, when do common ownership and control exist?
A. With respect to affiliated entities, common ownership exists if one of the involved organizations owns at least 5% of another organization. Common control means an organization has the power to significantly influence or direct the actions or policies of another organization.
Q. What makes an organization a hybrid entity?
A. A hybrid entity is an organization that performs some healthcare-related activities, but they aren't its primary business. If an organization elects to consider itself a hybrid entity, only its healthcare department is subject to the Security Standards.

Q. What is an organized healthcare arrangement (OHCA)?
A. An OHCA may be formed among legally separate covered entities that integrate their clinical and administrative operations. OHCAs differ from affiliated covered entities in that they aren't necessarily related to each other through common ownership or control. An example of an OHCA is a healthcare system that includes different types of healthcare providers, such as a hospital or medical staff, an ambulatory surgery center, and so on.

Q. Is an independent contractor considered a business associate?
A. No. The term business associate doesn't include employees or independent contractors, volunteers, or other persons working under the covered entity's direct supervision.

Q. What if terminating a contract with a business associate poses a hardship for the organization?
A. If terminating the relationship due to a violation isn't possible or would cause significant hardship for the covered organization, it must report the situation to HHS.

Q. What is IIHI?
A. Individually identifiable health information (IIHI) includes health, financial, and demographic information, created or received by a covered entity, that identifies, or could identify, the individual who is the subject of the information and relates to one of the following: the past, present, or future physical or mental health of an individual; the provision of healthcare to an individual; or the past, present, or future payment for healthcare provided to an individual.

Q. What is e-PHI?
A. E-PHI (electronic protected health information) includes IIHI (not contained in certain education and employment records) maintained or transmitted in any type of electronic media, but doesn't include paper information transmitted by facsimile.

Q. What mediums are considered electronic media?
A. Electronic media means storage devices in computers (hard drives) and any removable or transportable digital memory medium such as magnetic tape or disk, optical disk, or digital memory card. It also includes transmission devices used to exchange e-PHI already in electronic storage. Transmission media include such things as the Internet, a company-to-company extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media from one location to another.

Q. How can PHI be de-identified?
A. There are two ways to de-identify healthcare information. The first method is to remove all unique identifiers from the record. The second way is to have a qualified statistician declare that the risk of reidentification is small or nonexistent.

Q. What unique identifiers must be removed to de-identify health information?
A. To de-identify PHI, a covered entity or business associate must remove all identifying characteristics, including such information as names and addresses, dates, social security numbers, medical record numbers, telephone and fax numbers, e-mail and other Internet addresses, health insurance numbers, and identifiable photographs. Other identifiers may include account numbers, vehicle identifiers, and driver's license numbers. Information relating to gender, race, ethnicity, and marital status isn't individually identifiable and doesn't have to be removed.
Q. Are all implementation specifications required?
A. No. Implementation specifications are either required or addressable. A covered organization must implement required specifications as part of its security programs, but it may review and decide on addressable specifications based on its needs and organizational makeup.

Q. What are the documentation specifications of the Security Standards?
A. Along with requiring compliance to address the vulnerabilities of electronic information systems, the Security Standards also impose documentation requirements. That is, every covered organization must implement policies and procedures to comply with HIPAA's safeguards; these policies must be retained for six years; they must be made available to those responsible for implementing the procedures described in the documentation; and an organization must review its documentation periodically in response to changes in its security environment and business operations.

Q. What tools can be used to ensure the integrity of electronic information?
A. Depending on an organization's identified level of security risk, it may use electronic mechanisms such as error-correcting memory, magnetic disk storage systems, digital signatures, or check-sum technology. These will help authenticate that e-PHI has not been altered or destroyed in an unauthorized manner.

Q. What emergency procedures should your company have in place?
A. In addition to regulating access to e-PHI under normal conditions, covered entities must have procedures in place to obtain needed electronic information during an emergency. Depending on the type of emergency, programmed access controls may not be operable, and access could be denied to even those cleared for it. Measures should be developed beforehand to help valid users gain access to critical systems during emergency conditions.

Q. What are some potential authentication systems that an organization may use?
A. Aside from unique user IDs, other systems a covered organization might use for authentication include a biometric identification system, a password system, a personal identification number, and telephone call-back or token systems.

Q. What general requirements of the Security Standards does an organization have to meet?
A. The general requirements of the Security Standards are to ensure the confidentiality, integrity, and availability of all e-PHI it creates, receives, maintains, or transmits; protect against reasonably anticipated threats or hazards to the security or integrity of its e-PHI; protect against any reasonably anticipated uses or disclosures of the e-PHI that aren't required or permitted under the Privacy Standards; and ensure its workforce complies with its security policies and procedures.

Q. How can the workforce security standard's specifications be implemented?
A. The addressable implementation specifications are authorization and supervision, workforce clearance procedures, and termination procedures. The authorization and supervision specification instructs organizations to decide whether they should supervise employees who work with e-PHI or those locations where e-PHI might be accessed. Workforce clearance procedures direct organizations to consider whether they should assign certain access privileges to employees. Termination procedures describe how to discontinue an employee's ability to access e-PHI when he leaves the company.

Q. Who must participate in security awareness training?
A. All staff members of a covered organization, including management, must participate in the training under this standard. The content of the training may be tailored to an employee's functions. At a minimum, however, an organization must consider whether its training materials should include information relating to four implementation specification topics, all of which are addressable: security reminders; procedures for guarding against malicious software; procedures for monitoring login attempts and reporting login discrepancies; and procedures for creating, changing, and safeguarding passwords.
Q. **Must the evaluation of an organization’s security safeguards be conducted by an external entity?**

A. The evaluation doesn’t have to be conducted by an external entity. Staff trained to critique both the technical and nontechnical components of the organization's security plan can perform the evaluation.

Q. **What if the covered organization isn't the only occupant in a building?**

A. A facility security plan should take situations into account where a covered organization isn't the sole occupant of a building. When appropriate, an organization's security plan may include measures that would be taken by a third party or other occupant of a building to protect the physical security of the building.
### Questions

What must the safeguards that a covered entity implements do to meet the Security Standards?

*Check all that apply.*

- [x] Ensure the confidentiality, integrity, and availability of all e-PHI it creates, transmits, receives, or maintains.
- [x] Protect against reasonably anticipated threats or hazards to its e-PHI and against any reasonably anticipated use not allowed by the Privacy Standards.
- [ ] Cover both paper and electronic records.
- [x] Ensure its workforce will comply with its security policies and procedures.

---

### Feedback

The first, second, and fourth boxes should be checked.

The Security Standards require an entity to implement reasonable and appropriate administrative, physical, and technical safeguards. It must protect against reasonably anticipated threats to the security or integrity of its e-PHI, ensure its workforce complies with its security policies and procedures, and ensure the confidentiality, integrity, and availability of all e-PHI it handles. The Security Standards only apply to e-PHI and not to oral information or information on paper. However, the Privacy Standards apply to all information, whether in electronic form or not.

---

Davis Eye Care, a large ophthalmology group practice, submits claims for its services electronically. Once a year, it hires a coding and billing consultant to audit its claims to ensure the practice is billing for its services accurately. In order to perform the audit, the consultant requires the clinical and billing records for a sample of services furnished by the practice to patients. The practice provides the patient information to the consultant electronically.

Is the consultant considered a business associate under Privacy and Security Standards?

- [x] Yes
- [ ] No

Because the coding consultant is performing a service on Davis Eye Care's behalf that requires the use of e-PHI, the consultant would be considered a business associate under both the Privacy Standards and the Security Standards.
### Self-Check - Answers

#### Questions

Dr. Martin is an internist in Albany, New York. One of his patients, Steve, gets sick while visiting New York City and has some laboratory tests done while he's there. The lab then faxes the results to Dr. Martin.

Which of the following statements is true in this situation?

- [ ] The Security Standards apply because the lab tests are PHI.
- [ ] The Security Standards apply because the lab results identify Steve and discuss his condition.
- [x] The Security Standards don't apply because the lab tests were faxed to Dr. Martin.
- [ ] The Security Standards don't apply because Steve is Dr. Martin's patient.

Dr. Sanchez is a sole practitioner and a covered entity. She employs two people, as her medical technicians and to handle office administration. The workforce security standard has an addressable implementation specification (called workforce clearance procedure) suggesting that she limit her employees' e-PHI access to what their jobs require. Nevertheless, she decides—and documents the reason for her decision—not to grant varying levels of access to e-PHI, because both employees require equal access. However, Dr. Sanchez's practice is growing.

What should she do when she hires a new employee?

- [ ] Continue with the same practices without making policy changes.
- [x] Review her decision regarding the addressable specification.
- [ ] Stop accepting patients now to keep the practice small.
- [ ] Hire a clearinghouse to handle the e-PHI.

The access controls standard requires users to be assigned unique names or numbers for access control and tracking purposes.

- [x] True
- [ ] False

#### Feedback

The Security Standards don't apply to the lab results because they were faxed, and the standards only apply to e-PHI, which doesn't include paper information transmitted by facsimile. Just because the lab tests are PHI, and identify Steve, doesn't mean the Security Standards apply. The fact that Steve is Dr. Martin's patient is irrelevant to the Security Standards.

The Security Standards would require Dr. Sanchez to revisit her decision regarding the addressable specification. And if her growing practice required that she hire several more employees, she'd even more likely have to implement varying levels of access to e-PHI.

To comply with the access control standard, a covered entity must assign unique names or numbers to users of its electronic information so they may be identified when attempting to access e-PHI and tracked throughout their sessions.
# Self-Check - Answers

## Questions

According to the technical safeguards, which of the following is true? *Check all that apply.*

- [ ] The authentication standard requires unique user IDs.
- [ ] The transmission standard has two required implementation specifications.
- [ ] Organizations should consider addressable transmission issues and implementing measures to prevent e-PHI from being modified improperly.
- [ ] The goal of the integrity standards is to assure organizations that the data they make decisions on is intact.

---

New Point Ambulatory Surgery Center employs 25 people in various roles. Some of the employees are clinical staff, such as the operating room nurses, and others perform only administrative duties. New Point has a policy that only members of its billing office may process patient accounts. Nevertheless, the New Point security officer discovers, during his security risk analysis, that some employees who are not billing staff have accessed patient financial records to determine patients' copayment or deductible obligations.

Will the security officer find that the center is in compliance with HIPAA's Privacy and Security Standards?

- [ ] Probably
- [x] Probably not

---

ABC Clearinghouse takes pride in its security policies and its well-trained staff. To help ensure that its staff is properly trained in security measures, which of the following could this clearinghouse include in every staff member's training materials? *Check all that apply.*

- [x] Security reminders
- [x] Procedures for guarding against malicious software
- [ ] Procedures for reporting login discrepancies
- [ ] Procedures for safeguarding passwords

---

## Feedback

The first, third, and fourth boxes should be checked.

There are no required implementation specifications for the transmission standard; however, organizations are expected to consider addressable issues. The authentication standard requires organizations to implement systems to verify the identity of users attempting to access e-PHI, which includes unique user IDs. The integrity standard requires an organization to protect e-PHI from improper alteration or destruction. The goal of this standard is to assure covered entities that their data hasn't been altered or destroyed in an unauthorized manner.

The security officer should recognize that the employees’ actions violate New Point's policies required by the Privacy Standards, increasing the risk that an employee unfamiliar with the database could alter the financial information unknowingly. The officer may then decide that it's reasonable and appropriate to assign passwords to each of the clinical staff that limit their access to patient medical records and clinical databases.

All four boxes should be checked.

All staff members of a covered entity must participate in security awareness training. Covered entities must consider whether their training manuals should include information relating to security reminders; procedures for guarding against, detecting, and reporting malicious software; procedures for monitoring login attempts and reporting login discrepancies; and procedures for creating, changing, and safeguarding passwords.
Self-Check - Answers

Questions

Fern Landing, a skilled nursing facility, has workstations positioned throughout the facility. Some of the workstations are located in offices, but most are found on the nursing units and are accessible to all residents and their visitors.

What can Fern Landing do to protect the e-PHI it handles?

- [ ] Require photo identification from all visitors to the center.
- [ ] Require residents to sign a confidentiality agreement.
- [-] Create an automatic logoff for all computers.
- [ ] Discontinue all visiting hours.

Feedback

Because the public can easily view the workstations, Fern Landing should make it mandatory that all workstations have an automatic logoff. Requesting photo identification of all visitors won’t prevent them from viewing confidential information. As the residents don’t need to see the e-PHI, it won’t matter if they sign confidentiality agreements, and refusing visitors isn’t feasible.