PRACTICAL GUIDE SERIES

Chapter 6

Physical Safeguard Standards:

HIPAA Security Rule

What You Will Learn in This Chapter

- Specifics of the four Physical Safeguard Standards and their ten Implementation Specifications.
- How to distinguish *required* and *addressable* Implementation Specifications in Physical Safeguard Standards.
- How *reasonable* and *appropriate* actions provide the framework for a dental practice's implementation of Physical Safeguards, taking into account the dental practice's size, complexity, and environment in which it operates.
- Why maintenance of electricity is such a key element of the Security Rule's Physical Safeguard Standards.
- How to make electronic protected health information "unusable, unreadable, or indecipherable to unauthorized users" under the Breach Notification Rule.

Key Terms

The following terms are key to understanding the content of this chapter.
You will find meanings of each term in the Definitions of Key Terms in Appendix 1-1 and 1-2.

Access Control
Addressable
Authentication
Availability
Breach
Business Associate
Confidentiality
Contingency Operations
Covered Entity
Electricity Supply
Electronic Media
Electronic Protected Health Information
Encryption
Guidance
Implementation Specification
Integrity
Maintenance Records
NIST Guidelines
Protected Health Information
Required
Security Incident
Workstation

Chapter 6

Physical Safeguard Standards: HIPAA Security Rule

The HIPAA Security Physical Safeguard Standards are designed to help your dental practice protect your investment in the facilities and workstations that contain your *electronic* protected health information. The Physical Safeguards are defined in the HIPAA Security Rule as "physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[1]

Just as you lock doors to protect your physical assets, the HIPAA Security Rule requires you to take various steps to protect your electronic systems and the electronic protected health information contained therein. In addition, as prudence dictates in any business situation, HIPAA Security requires you to establish plans to handle contingencies in the event of an emergency or a disaster. Just as with Administrative and Technical Safeguards, the Physical Safeguards are used to protect the *confidentiality*, *integrity*, and *availability* of your dental practice's electronic protected health information.

Confidentiality, integrity, and availability are essential to privacy and security under HIPAA:

- *Confidentiality* means that data or information is not made available to or disclosed to unauthorized persons or processes.
- *Integrity* means that data or information has not been altered or destroyed in an unauthorized manner.
- *Availability* means that data or information is accessible and useable upon demand by an authorized person.

As your dental practice meets the requirements of the Physical Safeguard Standards, remember to keep in mind *confidentiality*, *integrity*, and *availability*.

There are four Physical Safeguard Standards: facility access controls, workstation use, workstation security, and device and media controls. Each Standard has Implementation Specifications, which can be *required* or *addressable*. Addressable does not mean "optional." Rather, an addressable Implementation Specification means that a dental practice must assess whether the Implementation Specification is a reasonable and appropriate safeguard for that dental practice, when analyzed with reference to its likely contribution to protecting the entity's electronic protected health information. Then the dental practice must either implement the Implementation Specification if it is reasonable and appropriate, or, if it is not reasonable and appropriate, the practice must document why not, implement an equivalent alternative measure if reasonable and appropriate, and document the equivalent alternative measure.

[1] 45 CFR 164.304.

As we mentioned in Chapters 4 and 5 in the discussion on Administrative and Technical Safeguards, respectively, whether your practice already has a comprehensive security strategy in place or is just beginning the process, it should have on hand as a resource the following 117-page publication from the National Institute of Standards and Technology (NIST):

> *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. NIST Special Publication 800-66 Revision 1, October 2008.[2]

We recommend that you download and read this document. We will refer to this document in the discussion that follows.

The Physical Safeguard Standards and their Implementation Specifications are listed in Table 6.1: Physical Safeguard Standards at a Glance. For each of the Physical Safeguard Standards, we provide in a footnote a specific reference in Appendix 6-1 to the "Physical Safeguards" page or pages in NIST Special Publication 800-66 Revision 1 that refer to that Standard. For example, NIST pages 35-36 outline and describe activities and sample questions that your dental practice should consider in addressing the Implementation Specifications for the first Standard discussed: Facility Access Controls, as shown in Table 6.1.

We also have provided you with ADA Tips along the way as we explore each of the Implementation Specifications of the Physical Safeguard Standards.

[2] This 117-page NIST document is available for download at: *www.csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf*. Appendix 6-1 includes information from this document relating to the Physical Safeguard Standards and their Implementation Specifications.

Table 6.1 Physical Safeguard Standards at a Glance

Security Standard	Implementation Specification	Required or Addressable
Facility Access Controls	i. Contingency Operations	Addressable
	ii. Facility Security Plan	Addressable
	iii. Access Control and Validation Procedures	Addressable
	iv. Maintenance Records	Addressable
Workstation Use		Required
Workstation Security		Required
Device and Media Controls	i. Disposal	Required
	ii. Media Re-Use	Required
	iii. Accountability	Addressable
	iv. Data Backup and Storage	Addressable

Like the Administrative and Technical Safeguards of the HIPAA Security Rule, Physical Safeguards focus on *electronic* protected health information. As a result, maintaining your electricity supply is a critical element of Physical Safeguard compliance and your dental practice's security strategy.

There are ten Implementation Specifications for the Physical Safeguard Standards. In our examination of several of these Implementation Specifications, we will discuss a document entitled *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, which is part of the Breach Notification Rule.[3] We will refer to this document as the "*Guidance*." Keep in mind that from time to time HHS may change the technologies and methodologies listed in the *Guidance*. The *Guidance* has implications for how your dental practice secures protected health information in electronic form and hard copy (paper or other physical items such as films), as well as how your practice secures portable electronic media such as portable data assistants (PDAs), tablets, notebooks, and laptops, whether these items are used **inside** or **outside** of your practice's premises. It also has implications for how your dental practice disposes of and reuses hardware and electronic media.

ADA® TIP

In reviewing the content and sample policies and procedures of the Physical Safeguard Standards and their Implementation Specifications, remember that your practice is entitled to use, and must document, *reasonable* and *appropriate* measures to comply with each standard.

[3] The *Guidance* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743 and is discussed further in this book in Chapter 1.

Standard: FACILITY ACCESS CONTROLS

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR[4] Part	Implementation Specification	Required or Addressable
Facility Access Controls	68 FR 8378 45 CFR 164.310(a)(1)	i. Contingency Operations ii. Facility Security Plan iii. Access Control and Validation Procedures iv. Maintenance Records	Addressable Addressable Addressable Addressable

What is Required: 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.[5]

What This Standard Means for Your Dental Practice:

This Standard requires a dental practice to establish policies and procedures to control access *to* and *within* the physical premises of the practice. Included in this Standard are requirements that your practice identify, authorize, and control who has access to your electronic information systems.

There are four Implementation Specifications for this Standard, all of which are addressable:[6]

- Contingency Operations.
- Facility Security Plan.
- Access Controls and Validation Procedures.
- Maintenance Records.

The Implementation Specifications are "applicable to an entity's business location or locations,"[7] and references to "the facility" mean "the physical premises and interior and exterior of the building,"[8] at each of the practice's locations.

The language of the following Implementation Specifications is straightforward. How the specifications are implemented depends on each dental practice's risk analysis, as discussed in Chapter 4, and other factors, including cost. In addressing these specifications, a dental practice should consider not only each specification individually, but also how they interrelate with Administrative and Technical Safeguards Implementation Specifications, especially with regard to the disaster recovery plan.

Many dental practices are small, with premises in single business dwellings or in multiple business office structures. Dental practices in a single business dwelling must implement the Standard so that the physical premises are protected. Dental practices in multiple business office structures must implement the Standard, taking into consideration, as the Covered Entity, that it "retains responsibility for considering facility security even where it shares space within a building with other organizations.

[4] *Code of Federal Regulations*
[5] Also see Appendix 6-1, *Facility Access Controls*, NIST pp.35-36.
[6] If an Implementation Specification is addressable, you must assess whether it is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, you must implement the specification. If the Implementation Specification is not reasonable and appropriate, you must implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.
[7] 68 *Federal Register* 8353.
[8] 68 *Federal Register* 8340.

Facility security measures taken by a third party must be considered and documented in the Covered Entity's facility security plan, when appropriate."[9]

If your dental practice is in a multiple business office structure, it should obtain a copy of the landlord's building security plan (and any subsequent updates or revisions) and include it as an exhibit in your practice's security plan. Reference the building security plan as your practice develops or amends its facility security policies and procedures.

Implementation Specification: Contingency Operations

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Facility Access Controls	68 FR 8378 45 CFR 164.310(a)(2)(i)	i. Contingency Operations	Addressable

What to Do:[10] Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

Sample Policy

Our dental practice Security Official is responsible for our disaster and emergency operations procedures, and in particular, building processes that are consistent with our Administrative Safeguard Standard Contingency Plan so that we can restore electronic systems and electronic protected health information in the event of a disaster or an emergency. Our dental practice workforce members are responsible for complying with the practice's contingency operations policies and procedures.

Sample Procedures

Our Security Official shall develop procedures to restore electronic systems and electronic protected health information should our dental practice experience a disaster or an emergency. Such procedures shall be based on outcomes of the practice's risk analysis, and coordinated with the Administrative Safeguard Standard, "Contingency Plan."

Our Security Official shall catalog the types of potential disasters and emergencies that could occur and determine their potential impact on the practice's operations. (For example, what would the practice do if the practice were damaged by fire? Would it relocate? How would it access backed up electronic protected health information? As another example, what will the practice do if its power supply is interrupted for a protracted period of time, or its electronic systems damaged by a lightning strike?)

Our Security Official shall outline procedures for re-establishing access to the practice's electronic systems and for restoring lost electronic protected health information and other business data. The procedures shall include identification of key personnel in the practice and personnel from our system vendors who would have emergency access credentials and responsibility for handling contingency operations.

[9] 68 *Federal Register* 8353.

[10] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

ADA TIP

The loss of electrical supply, even if unconnected with any other emergency or disaster, impairs access to *electronic* protected health information. At a minimum, a procedure for handling this contingency should be in place.

Implementation Specification: Facility Security Plan

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Facility Access Controls	68 FR 8378 45 CFR 164.310(a)(2)(ii)	ii. Facility Security Plan	Addressable

What to Do:[11] Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Sample Policy

Our dental practice will safeguard the practice and its facility and the electronic systems and electronic protected health information contained therein from unauthorized physical access, tampering, and theft.[12] Our dental practice workforce members are responsible for complying with the practice's facility security plan policies and procedures.

Sample Procedures

Our dental practice Security Official shall develop and evaluate the effectiveness of policies and procedures to protect the practice's facility[13] and the electronic systems and electronic protected health information contained therein. These policies and procedures will be based on our risk analysis of vulnerabilities and threats to our practice's physical infrastructure.

Our Security Official shall leverage the clinical and administrative assigned locations of workforce members to safeguard the practice internally during business hours.[14]

Our Security Official has determined that our dental practice's risk analysis will include consideration of the following areas for our development of policies and procedures to safeguard our practice's physical infrastructure:

- Which individuals should be authorized to access electronic systems containing electronic protected health information, and appropriate modes of access.

[11] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

[12] Be sure to include in your policy the potential for theft or loss of portable devices such as laptops, tablets, and portable data assistants (PDAs) that practitioners are increasingly using both inside and outside of the dental office. If these devices contain electronic protected health information, be sure to encrypt such information at rest and in motion. Appropriate procedures do not "preclude the use of electronic security systems in lieu of, or in combination with, physical security systems," on these devices or on others that are stationary in the practice facility. 68 *Federal Register* 8353.

[13] A practice in a single business dwelling may require an electronic security system to safeguard the facility and the electronic systems when no dental practice workforce members are on site (e.g., evenings and weekends). In a multiple business facility with an entrance guard on duty 24/7, the dental practice may just require strong locks on appropriate doors and windows.

[14] For example, in a small dental practice, the receptionist can play a key role in controlling access and ensuring that only authorized individuals have access to electronic systems that contain electronic protected health information.

- Procedures for opening and closing the dental office.
- Layout, design, and construction of our facility.
- Entrances and exits to our facility.
- Lock and key control.
- Locking mechanisms for doors, gates, windows, and other access points.
- Access badges and cards, and door keys.
- Sign-in and sign-out procedures.
- Person responsible for authorizing access to facility (e.g., Security Official).
- Parking rules.
- Surveillance of facility areas.
- Perimeter and barrier protection.
- Natural barriers, landscape, and terrain.
- Fencing, type and construction.
- Gate facilities and security checkpoints.
- Wall, ceiling, and floor construction.
- Identification and control of high-risk areas.
- Door and window locations and security devices used on each.
- Alarms, intrusion detection systems, and burglary deterrence devices.
- Fire and water hazards.
- Fire protection, detection, and extinguishers.
- Contingency operations, including emergency access for personnel to handle contingencies and emergencies.
- Reception area locations and facility entry controls.
- Employee surveillance and vigilance procedures.
- Access controls to locations containing electronic systems (e.g., server room).
- Firewalls safeguarding access to electronic protected health information.
- Environmental controls, such as heating, ventilation, and air conditioning, if necessary, for electronic systems.
- Plan for periodic testing, monitoring, and evaluating effectiveness of facility security.

Our Security Official shall make sure that the employee handbook includes the dental practice's facility security plan policies and procedures and that they are kept current.

ADA® TIP

Make sure that your practice secures your facility with an alert system that notifies the Security Official in the event of unauthorized access to the practice facility or any of its electronic systems.

Implementation Specification: Access Control and Validation Procedures

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Facility Access Controls	68 FR 8378 45 CFR 164.310(a)(2)(iii)	iii. Access Control and Validation Procedures	Addressable

What to Do:[15] Implement procedures to control and validate a person's access to facilities based on the person's role or function, including visitor control, and control of access to software programs for testing and revision.

Sample Policy

Our dental practice will control and validate a person's access to our facilities in the following four ways:

- Verify an individual's authorization — based on role or function — to access electronic systems that contain electronic protected health information.
- Establish a visitor sign-in/sign-out and badge system in order to safeguard electronic protected health information. Visitors, including Business Associates, shall be required to wear a "visitor" badge at all times while in the dental practice facility.
- Control access and movement within the dental practice.
- Escort visitors in areas with access to electronic protected health information if there is a reason for visitors to be in such areas.

Our dental practice workforce members are responsible for complying with the practice's access control and validation policies and procedures.

Sample Procedures

Our dental practice Security Official shall implement physical access controls for areas in our practice that have electronic systems that contain electronic protected health information[16] and shall be responsible for validating a person's access to such systems and information. The Security Official shall confirm that any outside party requiring access to the dental practice's electronic systems that contain electronic protected health information meets the following conditions: (a) Business Associate Agreement in place; (b) positive identification of appropriate credentials of any representative of the Business Associate; and (c) Business Associate representative is aware of and understands the dental practice's security policies and procedures.

Our Security Official shall confirm that all electronic systems containing electronic protected health information that are stationary in the practice are housed in physically secure locations within the practice, and that all portable electronic systems containing electronic protected health information that are used inside or outside of the practice are password protected with such information encrypted. Our Security Official shall assign facility keys and alarm system codes to designated dental practice workforce members. The Security Official shall implement and manage key assignments and

[15] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

[16] Such controls should include an intrusion alarm system to alert authorities and designated workforce members in the event of a break-in to the dental practice facility after hours of operation.

their locations so that keys are returned and lock and alarm codes changed when designated practice workforce members resign or are terminated, or other circumstances warrant. The Security Official shall verify any person who is not a member of our workforce who may have access to our electronic protected health information, especially representatives of electronic systems vendors who test, revise, and update systems hardware and software used in the dental practice, and notify them of our security policies and procedures. Our Security Official also shall obtain appropriate Business Associate Agreements and, in addition to a secure file of these agreements in the practice, maintain a duplicate file in a secure location off-site, such as with the practice attorney.

ADA® TIP

In a dental practice with a sole practitioner and only one employee to handle administrative duties, system access that is based on function and need may be broader than in a practice with multiple dentists and a large workforce.

Implementation Specification: Maintenance Records

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Maintenance Records	68 FR 8378 45 CFR 164.310(a)(2)(iv)	iv. Maintenance Records	Addressable

What to Do:[17] Implement 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).

Sample Policy

Our dental practice shall document repairs and modifications to the physical components of the practice's facility that are related to security, including hardware, locks, doors, and walls. Our dental practice workforce members are responsible for complying with the practice's maintenance records policies and procedures.

Sample Procedures

Our dental practice Security Official shall maintain a log of any repairs or modifications to the physical components of the practice's facility that are related to security. The log shall include: date of repair or modification; description of the reason for repair or modification; name, address, and contact telephone number of person or entity performing the modification; cost, if any, of the repair or modification; signature of Security Official or designated responsible workforce member responsible for making sure repair is completed.[18]

[17] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

[18] See Appendix 6-2 for sample form: *Maintenance Repair Log.*

Our Security Official shall update the log in writing within one business day of completion of any security-related repair or modification to the physical components of the practice's facility, and shall verify that the repair or modification was completed.

Our Security Official shall maintain the log, in print or electronic format, for a period of six years from the date of the last recorded security-related repair or modification to the physical components of the practice's facility or from the date when the last entry was last in effect, whichever is later.[19]

ADA TIP

Document your maintenance records and retain them as required by the HIPAA Security Rule. The U.S. Department of Health and Human Services' Office for Civil Rights (OCR), which is responsible for enforcing the HIPAA Privacy and Security Rules, may require such documentation as proof of your practice's compliance with those rules in the event of a compliance audit or a complaint investigation relating to a security incident or privacy breach.

Standard: WORKSTATION USE

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Workstation Use	68 FR 8378 45 CFR 164.310(b)		Required

What is Required: 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 protected health information.[20]

There is not a separate Implementation Specification for this Standard. Rather, the Implementation Specification for workstation use is specified in the language of the Standard and is thus required.

What This Standard Means for Your Dental Practice:

This safeguard Standard pertains to workstations that can access electronic protected health information. It requires your dental practice to account for appropriate workstation uses, to determine how such uses are to be performed, and to determine the physical environment in which access to electronic protected health information will be permitted. Workstations include, but are not limited to, desktop computers, laptop computers, tablet computers, personal data assistants (PDAs), and any other electronic media that transmit, receive, or store electronic protected health information.

[19] The HIPAA Security Rule permits electronic documentation, which should be routinely backed up.
[20] Also see Appendix 6-1, *Workstation Use*, NIST p. 37.

Examples of appropriate workstation use policies include:

- Workforce members never leave workstations unattended without first logging off.
- In a controlled access environment, workstations automatically log off in the absence of activity for a period of time, say, ten minutes or less.[21]
- Access to the Internet is controlled while working with electronic protected health information in order to minimize unauthorized access by outsiders to such information over an open network.

Clinical practitioners increasingly use devices such as PDAs (personal data assistants) and other small electronic media to connect to electronic records that may contain electronic protected health information. When considering workstation use, Security Officials in dental practices must broaden their focus to include these portable devices used inside or outside of the practice facility.

The Breach Notification Rule *Guidance*[22] specifies technologies and methodologies to "secure" electronic protected health information on these portable electronic media via encryption, so that such information is "unusable, unreadable, or indecipherable"[23] if the device is lost or stolen. If appropriate encryption is enabled on these devices and the devices are lost or stolen, then the practice may not be required to carry out the potentially time consuming and expensive breach notification requirements described in the Breach Notification Rule.[24]

Sample Policy

Our dental practice has specified the proper functions to be performed on each workstation, the manner in which they are to be performed, and the physical attributes of the surroundings of specific workstations or classes of workstations that can access electronic protected health information. Our dental practice workforce members are responsible for complying with the practice's workstation use policies and procedures.

Sample Procedures

Our Security Official shall establish and implement workstation use procedures and physical access controls for workstation areas in the practice that contain electronic protected health information.

Our Security Official, or appropriate designee, shall provide oversight for the following activities:

- No food or drink (if water, must have a screw-top lid) near workstations that contain electronic protected health information.
- Compliance with terms and conditions of software licenses and copyright laws.
- Workforce members routinely keep workstation antivirus software current when updates are routed to them.
- Place workstations containing electronic protected health information in controlled areas where only practice workforce member users and other authorized users, such as electronic system vendors under a Business Associate Agreement, have access, as appropriate.[25]

[21] Automatic logoff time is a control setting on most electronic media. As part of your practice's risk analysis, determine the appropriate period of time before automatic logoff. Consider the location of the electronic media, access to location by unauthorized persons, and size of practice.

[22] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743 and is discussed further in this book in Chapter 1. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[23] 45 CFR 164.402

[24] The Department of Health and Human Services will enforce the Breach Notification Rule for any breach discovered on or after Monday, February 22, 2010, but does not relieve a Covered Entity of responsibility for complying with the Breach Notification Rule from its effective date of September 23, 2009. Dental practices must also comply with breach notification requirements under any applicable state law.

[25] The workstation used by the receptionist is a highly vulnerable point of unauthorized access that should receive special attention. This workstation, and any other workstation containing electronic protected health information, should be shielded from patients and other passersby in the practice who are not authorized to have access to such information.

- Portable electronic media containing electronic protected health information, used in the practice or authorized in writing to be taken out of the practice, has appropriate encryption as outlined in the Breach Notification Rule *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.*[26]

ADA® TIP

Any portable workstation containing electronic protected health information, used in the practice or taken out of the practice by an authorized user, must have appropriate encryption to "secure" that information, as outlined in the Breach Notification Rule *Guidance*.

Standard: WORKSTATION SECURITY

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Workstation Security	68 FR 8378 45 CFR 164.310(c)		Required

What is Required: Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.[27]

There is not a separate Implementation Specification for this Standard. Rather, the Implementation Specification for workstation security is specified in the language of the Standard and is thus required.

What This Standard Means for Your Dental Practice:

This safeguard Standard requires your dental practice to secure workstations in such a manner that access is restricted to authorized users. The solution is "dependent on the [covered] entity's risk analysis and risk management process,"[28] and may involve controlled access to the workstation, and/or controls on the workstation, that prevent access by unauthorized users.

Examples of appropriate workstation security policies include:

- A requirement that workforce members never relocate workstations without authorization.
- A policy prohibiting workforce members from allowing patients or guests to enter nonpublic areas of the dental office where workstations with access to electronic protected health information are located.
- Training workforce members to implement traffic flow patterns that direct patients away from areas of the dental office containing workstations that have access to electronic protected health information.

[26] The *Guidance* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.
[27] Also see Appendix 6-1, *Workstation Security*, NIST p. 38.
[28] 68 *Federal Register* 8354.

Clinical practitioners increasingly use devices such as PDAs (personal data assistants) and other small electronic media to connect to electronic records that may contain electronic protected health information. When considering workstation security, Security Officials in dental practices must broaden their focus to include these portable devices used inside or outside of the practice facility.

The Breach Notification Rule *Guidance*[29] specifies technologies and methodologies to "secure" electronic protected health information on these portable electronic media via encryption, so that such information is "unusable, unreadable, or indecipherable"[30] to an unauthorized user. If appropriate encryption is enabled on these devices and the devices are lost or stolen, then the practice may not have to provide the potentially time consuming and expensive notifications described in the Breach Notification Rule.[31]

Sample Policy

Our dental practice will maintain workstation security for all workstations that provide access to electronic protected health information in order to prevent access by unauthorized users. Our dental practice workforce members are responsible for complying with the practice's workstation security policies and procedures.

Sample Procedures

Our dental practice Security Official shall establish and implement workstation security procedures and physical access controls to workstation areas in the practice.

Our Security Official shall assign passwords to authorized users of electronic media that contain electronic protected health information. Our Security Official shall establish the procedures that we determined were appropriate when we conducted our risk analysis. These procedures include ensuring that "strong" passwords are used, that they are changed regularly, and that their use is monitored.

Our Security Official shall periodically issue security reminders about the use of passwords, including reminders of the sanctions for sharing passwords and for inappropriately posting written passwords on workstations or desktop surfaces, or placing them under desktop calendars or in drawers.

Our Security Official shall verify that workstations containing electronic protected health information are placed in controlled areas where only practice workforce members who are authorized users, and other authorized users such as electronic system vendors under a Business Associate Agreement, have access, as appropriate.[32]

Our Security Official shall make sure that workstations that contain electronic protected health information are not visible to unauthorized passersby.

Our Security Official shall monitor unattended electronic media so that they have an automatic logoff of ten minutes or less, with the time to be determined through our practice's risk analysis.

Our Security Official shall validate a Business Associate's credentials before allowing access to electronic media that contain electronic protected health information.

[29] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743 and is discussed further in this book in Chapter 1. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[30] 45 CFR 164.402.

[31] The Department of Health and Human Services will enforce the Breach Notification Rule for any breach discovered on or after Monday, February 22, 2010. Covered Entities must also comply with any applicable state law requirements.

[32] The workstation used by the receptionist is a highly vulnerable point of unauthorized access in a dental practice and should receive special attention in the practice's risk analysis. This workstation, and any other workstation containing electronic protected health information, should be shielded from patients and from any other passersby who are not authorized to access such information.

Our Security Official shall oversee and confirm that any portable electronic media containing electronic protected health information, used in the practice or authorized in writing to be taken out of the practice, have appropriate encryption as outlined in the *Guidance* of the Breach Notification Rule.[33]

ADA® TIP

The Workstation Use and Workstation Security Physical Safeguard Standards are closely linked, with the goals of safeguarding electronic protected health information from unauthorized users. We reiterate the ADA Tip from the Workstation Use Standard discussion here because increasing use of portable workstation devices outside of the physical facility of the practice creates new vulnerabilities for your practice:

Any portable workstation containing electronic protected health information, used in the practice or taken out of the practice by an authorized user, must have appropriate encryption to "secure" that information, as outlined in the Breach Notification Rule *Guidance*.

Standard: DEVICE AND MEDIA CONTROLS

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Device and Media Controls	68 FR 8378 45 CFR 164.310(d)(1)	i. Disposal ii. Media Re-use iii. Accountability iv. Data Backup and Storage	Required Required Addressable Addressable

What is Required: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within a facility.[34]

What This Standard Means for Your Dental Practice:

This Standard requires your dental practice to establish policies and procedures that track the receipt and removal of hardware and electronic media that contain electronic protected health information that come into your dental practice and leave the practice, and to control the movement of hardware and electronic media within the practice. The policies and procedures will be based on your practice's risk analysis.

[33] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770); it appears at 74 *Federal Register* 42742-42743. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[34] Also see Appendix 6-1, *Device and Media Controls*, NIST p. 39.

At a minimum, your dental practice should create (and continuously update) an inventory of all practice hardware and electronic media; track the movement of inventory within the practice; and control introduction of unauthorized electronic media, such as software, DVDs, and flash drives brought into the practice by a workforce member. Maintaining an up-to-date inventory enhances your practice's ability to mitigate risk in the event of a contingency such as the introduction of a virus that corrupts your practice's network.

There are four Implementation Specifications for this Standard: two are required and two are addressable, as noted here:

i. Disposal (Required)

ii. Media Re-use (Required)

iii. Accountability (Addressable)

iv. Data Backup and Storage (Addressable)

With respect to the two required Implementation Specifications (disposal and media re-use), it is important to remember that *file deletion* and *erasure* commands or functions generally do not delete files and data, but rather delete only the file name but not the underlying data content. Hence, using these functions prior to disposal or media re-use may not achieve the intended result: namely, elimination of electronic protected health information and proprietary business information of your practice. If you dispose of or reuse electronic media, ask your vendor or computer store how to delete electronic protected health information and how to *verify* the deletion.

As mentioned earlier in this chapter, the Breach Notification Rule *Guidance*[35] provides instructions on how to "secure" electronic protected health information by making it "unusable, unreadable, or indecipherable."[36] If *secured* electronic protected health information is breached, the Covered Entity may not have to send out notifications under the Breach Notification Rule. The *Guidance* states that protected health information stored or recorded on electronic media can be secured by clearing, purging, or destroying the electronic media consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization*,[37] such that the PHI cannot be retrieved.[38]

Make sure that your practice's system vendors are aware of and understand the NIST disposal requirements for electronic media that contain electronic protected health information.

Sample Policy

Our dental practice will monitor and document the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of our facility, and the movement of hardware and electronic media within the facility. Our dental practice workforce members are responsible for complying with the practice's device and media controls policies and procedures.

[35] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743 and is discussed further in this book in Chapter 1. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[36] 45 CFR 164.402.

[37] Richard Kissel, Matthew Scholl, Steven Skolochenko, and Xing Li, *Guidelines for Media Sanitization*, NIST Special Publication 800-88, September 2006, which is available online at: *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf*.

[38] 74 *Federal Register* 42742-42743.

Sample Procedures

Our dental practice Security Official shall establish and implement media control policies and procedures, including identifying and tracking all hardware and electronic media used in our practice.

Our Security Official shall train our workforce members to protect hardware and electronic media so as to protect our practice's electronic protected health information and proprietary business information from loss and from exposure to unauthorized persons.

Our Security Official, in conjunction with our IT personnel, shall prohibit the use of unauthorized hardware and electronic media within the practice, and shall enforce sanctions for violations of this procedure.

Our Security Official shall verify that electronic protected health information is backed up on a routine basis and stored off-site in a physically secure facility. The Security Official shall verify on a regular basis that an exact copy of such information is readily retrievable.

Our Security Official shall confirm that any disposal of hardware or electronic media complies with the Breach Notification Rule *Guidance*[39] and NIST guidelines so that any electronic protected health information on such hardware or electronic media is "unusable, unreadable, or indecipherable" and cannot be retrieved.

ADA TIP

The Breach Notification Rule Guidance must be considered in a reexamination of your dental practice's risk analysis regarding the Implementation Specifications of this Device and Media Controls Physical Safeguard Standard.

[39] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

Implementation Specification: Disposal

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Device and Media Controls	68 FR 8378 45 CFR 164.310(d)(2)(i)	i. Disposal	Required

What to Do: Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Sample Policy

Prior to final disposition of any hardware or electronic media in our practice, our practice will dispose of electronic protected health information in a manner that is consistent with the Breach Notification Rule *Guidance*.[40] Our dental practice workforce members are responsible for complying with the practice's hardware and electronic media disposal policies and procedures.

Sample Procedures

Our dental practice Security Official shall confirm that our practice's hardware and electronic media disposal procedures are consistent with the Breach Notification Rule *Guidance* and any updates to it, and that our system vendors are aware of and understand the National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization*,[41] which is the current *Guidance*-recommended set of guidelines for disposal of electronic media containing electronic protected health information.[42]

Our Security Official shall include the NIST *Guidelines* in our risk analysis updates and review.

Our Security Official shall verify that any electronic protected health information is deleted from hardware or electronic media.

ADA® TIP

When your dental practice updates its risk analysis, make sure to review the Breach Notification Rule *Guidance* and NIST *Guidelines* to determine whether your electronic protected health information is "secured" with respect to disposal of hardware and electronic media. If not, make it part of your risk analysis to weigh the cost of securing your electronic protected health information against the cost of complying with the notification requirements under the Breach Notification Rule.

[40] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[41] Available online at: *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf*.

[42] 74 *Federal Register* 42743.

Implementation Specification: Media Re-Use

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Device and Media Controls	68 FR 8378 45 CFR 164.310(d)(2)(ii)	ii. Media Re-Use	Required

What to Do: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Sample Policy

Our dental practice Security Official shall confirm that our practice's hardware and electronic media disposal procedures are consistent with the Breach Notification Rule *Guidance*[43] and any updates to it, and that our system vendors are aware of and understand the National Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization*,[44] which is the current *Guidance*-recommended set of guidelines for removal of electronic protected health information on electronic media "such that the PHI cannot be retrieved." Our dental practice workforce members are responsible for complying with the practice's hardware and electronic media re-use policies and procedures.

Sample Procedures

Our Security Official shall include the NIST *Guidelines* in our risk analysis updates and review.

Our Security Official shall verify that any electronic protected health information is removed from electronic media "such that the PHI cannot be retrieved."

Our Security Official has determined that electronic media are relatively inexpensive and are becoming more so each year. Accordingly, as a result of our practice's risk analysis, we consider it appropriate risk mitigation to destroy rather than re-use electronic media (we balanced cost of new electronic media against potential costs of access of electronic protected health information by unauthorized users).

ADA® TIP

The Breach Notification Rule imposes notification requirements on Covered Entities that discover a breach of unsecured PHI. Weigh the burden of the notification requirements against the cost of securing PHI according to the Breach Notification *Guidance* and NIST *Guidelines* when you conduct an initial or updated HIPAA Security risk analysis, and whenever you consider reusing or replacing your hardware and electronic media.

[43] The *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* is part of the "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," published on August 24, 2009 (74 *Federal Register* 42739-42770). The *Guidance* appears at 74 *Federal Register* 42742-42743 and is discussed further in this book in Chapter 1. HHS may change the technologies and methodologies listed in the *Guidance* from time to time.

[44] Available online at: *http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.*

Implementation Specification: Accountability

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Device and Media Controls	68 FR 8378 45 CFR 164.310(d)(2)(iii)	iii. Accountability	Addressable

What to Do:[45] Maintain a record of the movements of hardware and electronic media and any person responsible therefor.[46]

Sample Policy

Our dental practice will establish and maintain a written record of the movements of hardware and electronic media and any person responsible therefor. Our dental practice workforce members are responsible for complying with the practice's accountability policies and procedures.

Sample Procedures

Our dental practice Security Official shall establish and maintain documentation of the movement of hardware and electronic media and the parties responsible for such hardware and electronic media. The documentation should include the following column headings: Description; Model; Serial Number; Manufacturer; Purchase Price; Date Purchased; Date in Service; Assigned to; Reassigned to; Date Taken Out of Service.[47]

Our Security Official shall maintain the documentation "for six years from the date of its creation or the date when it last was in effect, whichever is later."[48]

Our Security Official shall maintain an up-to-date copy of the inventory in a safe place outside of the premises of the practice, such as in a safe deposit box, or with our practice's attorney, bookkeeper, or insurance agent.

ADA® TIP

Your dental practice should maintain in a secure location an electronic copy of your inventory of hardware and electronic media indicating its deployment in your practice. Such an inventory should be accessible, and would be useful in the event of a disaster or an emergency.

[45] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

[46] Dental practices with one or two dentists and small workforces should focus on the flexibility of this Implementation Specification. This Implementation Specification recognizes that "small providers would be unlikely to be involved in large-scale moves of equipment that would require systematic tracking, unlike, for example, large healthcare providers or health plans." 68 *Federal Register* 8354.

[47] See Appendix 6-3 for form: Sample *Electronic Media and Hardware Movement Log.*

[48] 45 CFR 164.316(b)(2)(i).

Implementation Specification: Data Backup and Storage

Physical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Device and Media Controls	68 FR 8378 45 CFR 164.310(d)(2)(iv)	iv. Data Backup and Storage	Addressable

What to Do:[49] Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Sample Policy

Our dental practice will regularly back up electronic protected health information, in accordance with the backup procedures that we determined were appropriate when we conducted our risk analysis. We will keep an exact copy of that information stored off-site and readily retrievable in case it is needed. Prior to moving stationary hardware or electronic media in the practice's facility, we will back up the electronic protected health information and verify that it is an exact copy. Our dental practice workforce members are responsible for complying with the practice's data backup and storage policies and procedures.

Sample Procedures

Our dental practice Security Official shall confirm that a retrievable, exact copy of electronic protected health information is available prior to movement of stationary hardware or electronic media in the practice.

Our Security Official shall periodically test the practice's data backup procedures, with the frequency that we determined was appropriate when we conducted our practice's risk analysis.

Our Security Official shall confirm that backup data are tested for integrity and availability, with the frequency that we determined was appropriate when we conducted our practice's risk analysis.

Our Security Official shall confirm that the practice maintains and stores off-site, at a secure facility daily, weekly, monthly, and quarterly backups of the practice's electronic protected health information, software, and system audits.

ADA TIP

Make sure that your practice maintains daily, weekly, monthly, and quarterly encrypted backups of the practice's electronic protected health information, software, and system audits, and stores them off-site at a secure facility.

[49] This Implementation Specification is addressable. Assess whether the Implementation Specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then implement the specification. If the Implementation Specification is not reasonable and appropriate, implement an equivalent alternative measure if it is reasonable and appropriate. Document your decision and your reasoning for whatever your practice implements.

Appendix 6-1
NIST Activities and Sample Questions Regarding Physical Safeguards

NIST Special Publication 800-66 Revision 1

National Institute of Standards and Technology
U.S. Department of Commerce

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

**Matthew Scholl, Kevin Stine,
Joan Hash, Pauline Bowen, Arnold Johnson,
Carla Dancy Smith, and Daniel I. Steinberg**

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

4.10. Facility Access Controls (§ 164.310(a)(1))[60]

HIPAA Standard: *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*

Key Activities	Description	Sample Questions
1. Conduct an Analysis of Existing Physical Security Vulnerabilities[61, 62]	• Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. • Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed. • Determine which types of facilities require access controls to safeguard EPHI, such as: ○ Data Centers ○ Peripheral equipment locations ○ IT staff offices ○ Workstation locations.	• If reasonable and appropriate, do nonpublic areas have locks and cameras? • Are workstations protected from public access or viewing?[63] • Are entrances and exits that lead to locations with EPHI secured? • Do policies and procedures already exist regarding access to and use of facilities and equipment? • Are there possible natural or man-made disasters that could happen in our environment?[64] • Do normal physical protections exist (locks on doors, windows, etc., and other means of preventing unauthorized access)?
2. Identify Corrective Measures[65, 66]	• Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure that proper access is allowed. • Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed.	• Who is responsible for security?[67] • Is a workforce member other than the security official responsible for facility/physical security? • Are facility access control policies and procedures already in place? Do they need to be revised? • What training will be needed for employees to understand the policies and procedures?[68] • How will we document the decisions and actions?[69] • Are we dependent on a landlord to make physical changes to meet the requirements?

[60] Note: See also Section 4.10, *HIPAA Standard: Facility Access Controls* and Section 4.14, *HIPAA Standard: Access Controls.*
[61] This key activity may be performed as part of the risk analysis implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process.*
[62] See Key Activity 4.10.3, *Develop a Facility Security Plan.* This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.
[63] See Section 4.11, *HIPAA Standard: Workstation Use.*
[64] See Section 4.7, *HIPAA Standard: Contingency Plan.*
[65] This key activity may be performed as part of the risk management implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process.*
[66] See Key Activity 4.10.3, *Develop a Facility Security Plan.* This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.
[67] See Section 4.2, *HIPAA Standard: Assigned Security Responsibility.*
[68] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

Key Activities	Description	Sample Questions
3. Develop a Facility Security Plan **Implementation Specification (Addressable)**	• *Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.* • Implement appropriate measures to provide physical security protection for EPHI in a covered entity's possession. • Include documentation of the facility inventory, as well as information regarding the physical maintenance records and the history of changes, upgrades, and other modifications. • Identify points of access to the facility and existing security controls.	• Is there an inventory of facilities and existing security practices? • What are the current procedures for securing the facilities (exterior, interior, equipment, access controls, maintenance records, etc.)? • Is a workforce member other than the security official responsible for the facility plan? • Is there a contingency plan already in place, under revision, or under development?[70]
4. Develop Access Control and Validation Procedures **Implementation Specification (Addressable)**	• *Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.* • Implement procedures to provide facility access to authorized personnel and visitors, and exclude unauthorized persons.	• What are the policies and procedures in place for controlling access by staff, contractors, visitors, and probationary employees? • How many access points exist in each facility? Is there an inventory? • Is monitoring equipment necessary?
5. Establish Contingency Operations Procedures **Implementation Specification (Addressable)**	• *Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.*	• Who needs access to EPHI in the event of a disaster? • What is the backup plan for access to the facility and/or EPHI? • Who is responsible for the contingency plan for access to EPHI? • Who is responsible for implementing the contingency plan for access to EPHI in each department, unit, etc.? • Will the contingency plan be appropriate in the event of all types of potential disasters (fire, flood, earthquake, etc.)?
6. Maintain Maintenance Records **Implementation Specification (Addressable)**	• *Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).*	• Are records of repairs to hardware, walls, doors, and locks maintained? • Has responsibility for maintaining these records been assigned?

[69] See Section 4.22, *HIPAA Standard: Documentation.*
[70] See Section 4.7, *HIPAA Standard: Contingency Plan.*

4.11. Workstation Use (§ 164.310(b))

HIPAA Standard: *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 protected health information.*

Key Activities	Description	Sample Questions
1. Identify Workstation Types and Functions or Uses	• Inventory workstations and devices. • Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues. • Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.	• Do we have an inventory of workstation types and locations in my organization? • Who is responsible for this inventory and its maintenance? • What tasks are commonly performed on a given workstation or type of workstation? • Are all types of computing devices used as workstations identified along with the use of these workstations?
2. Identify Expected Performance of Each Type of Workstation	• Develop and document policies and procedures related to the proper use and performance of workstations.	• How are workstations used in day-to-day operations? • What are key operational risks that could result in a breach of security?
3. Analyze Physical Surroundings for Physical Attributes[71]	• Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts. • Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and dispose of sensitive information as needed.	• Where are workstations located? • Is viewing by unauthorized individuals restricted or limited at these workstations? • Do changes need to be made in the space configuration? • Do employees understand the security requirements for the data they use in their day-to-day jobs?

[71] See Section 4.5, *HIPAA Standard: Security Awareness and Training.* This key activity should be performed during security training or awareness activities.

4.12. Workstation Security (§ 164.310(c))

HIPAA Standard: *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*

Key Activities	Description	Sample Questions
1. Identify All Methods of Physical Access to Workstations	• Document the different ways workstations are accessed by employees and nonemployees.	• Is there an inventory of all current workstation locations? • Are any workstations located in public areas? • Are laptops used as workstations?
2. Analyze the Risk Associated with Each Type of Access[72]	• Determine which type of access holds the greatest threat to security.	• Are any workstations in areas that are more vulnerable to unauthorized use, theft, or viewing of the data they contain? • What are the options for making modifications to the current access configuration?
3. Identify and Implement Physical Safeguards for Workstations	• Implement physical safeguards and other security measures to minimize the possibility of inappropriate access to EPHI through workstations.	• What safeguards are in place, i.e., locked doors, screen barriers, cameras, guards?[73] • Do any workstations need to be relocated to enhance physical security? • Have employees been trained on security?[74]

[72] This key activity may be conducted pursuant to the risk analysis and risk management implementation specifications of the security management process standard. See Section 4.1, *HIPAA Standard: Security Management Process.*
[73] See Section 4.1, *HIPAA Standard: Security Management Process.*
[74] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

4.13. Device and Media Controls (§ 164.310(d)(1))

HIPAA Standard: *Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.*

Key Activities	Description	Sample Questions
1. Implement Methods for Final Disposal of EPHI **Implementation Specification (Required)**	• *Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.* • Determine and document the appropriate methods to dispose of hardware, software, and the data itself. • Assure that EPHI is properly destroyed and cannot be recreated.	• What data is maintained by the organization, and where? • Is data on removable, reusable media such as tapes and CDs? • Is there a process for destroying data on hard drives and file servers? • What are the options for disposing of data on hardware? What are the costs?
2. Develop and Implement Procedures for Reuse of Electronic Media **Implementation Specification (Required)**	• *Implement procedures for removal of EPHI from electronic media before the media are made available for reuse.* • Ensure that EPHI previously stored on electronic media cannot be accessed and reused. • Identify removable media and their use. • Ensure that EPHI is removed from reusable media before they are used to record new information.	• Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? • Is one individual and/or department responsible for coordinating the disposal of data and the reuse of the hardware and software? • Are employees appropriately trained on security and risks to EPHI when reusing software and hardware?[75]
3. Maintain Accountability for Hardware and Electronic Media **Implementation Specification (Addressable)**	• *Maintain a record of the movements of hardware and electronic media and any person responsible therefore.* • Ensure that EPHI is not inadvertently released or shared with any unauthorized party. • Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with EPHI.	• Where is data stored (what type of media)? • What procedures already exist regarding tracking of hardware and software within the company? • If workforce members are allowed to remove electronic media that contain or may be used to access EPHI, do procedures exist to track the media externally? • Who is responsible for maintaining records of hardware and software?
4. Develop Data Backup and Storage Procedures **Implementation Specification (Addressable)**	• *Create a retrievable exact copy of EPHI, when needed, before movement of equipment.* • Ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of EPHI during equipment relocation.	• Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing EPHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?

[75] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*

Appendix 6-2
Sample Facility Maintenance Repair Log

Use this form to maintain a log of repairs that are made to ensure your physical location is secure.

Name of Practice _____

Facility Address _____ City _____ State _____ Zip _____

Description of Repair	Date Scheduled	Date Repaired	Contractor		Cost	Approval[1]
			Name, Address	Phone		

[1] Security Official or appointed representative should initial when the repair has been completed.

Appendix 6-3
Sample Electronic Media and Hardware Movement Log

Use this form to check out and track the location of electronic media such as portable computers. You do not need to check out handheld devices or smart phones, but laptops, and back up disks must be logged in and out.

Name of Practice _____

Facility Address _____ City _____ State _____ Zip _____

Workstation	Static IP Address	Assigned User		Check Out		Initials
		Name	Location	Out	In	

[1] Security Official or appointed representative should initial when the repair has been completed.