PRACTICAL GUIDE SERIES

Chapter 5

Technical Safeguard Standards:

HIPAA Security Rule

What You Will Learn in This Chapter

- Specifics of five Technical Safeguard Standards and their ten Implementation Specifications.
- How to distinguish *required* and *addressable* Implementation Specifications in Technical Safeguard Standards.[1]
- How *reasonable* and *appropriate* actions provide the framework for a dental practice's implementation of Technical Safeguards, based on the dental practice's size, complexity, and environment in which it operates.
- How to "secure" electronic protected health information by making it "unusable, unreadable, or indecipherable to unauthorized individuals."[2]

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
Access Control
Audit Controls
Audit Trail
Authentication
Availability
Breach
Confidentiality
Covered Entity
Data Authentication
Decryption
Electronic Protected Health Information
Electronic Storage Media
Emergency Access
Encryption
Implementation Specification
Information System
Integrity
Password
Protected Health Information
Security Incident
Technical Safeguards
Unsecured Protected Health Information
User
User Identity or User ID
Workstation

[1] For a particular safeguard standard, a *required* Implementation Specification requires implementation by the dental practice, whereas an *addressable* Implementation Specification requires the dental practice to determine the reasonableness and appropriateness of the Implementation Specification, and implement it if it is reasonable and appropriate; if not, implement an equivalent alternative measure that would be reasonable and appropriate. In either case, the dental practice will base its decision on outcomes of its risk analysis, and is required to document its decision-making.
[2] 74 *Federal Register* 42742.

Chapter 5

Technical Safeguard Standards:[3] HIPAA Security Rule

Dental practices have been required to comply with Administrative, Technical, and Physical Safeguards since April 21, 2005.

HITECH Update. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act on February 17, 2009, requires *Business Associates* of dental practices to comply with the HIPAA Security Rule safeguards, beginning February 17, 2010.

The HITECH Act and the HHS Breach Notification Rule impose reporting requirements on dental practices for a breach of unsecured protected health information. Federal enforcement of reporting requirements began on February 22, 2010, for breaches discovered on or after that date. Dental practices and their Business Associates may also be subject to enforcement of applicable state laws regarding breach notification for breaches discovered prior to, on, or after that date.

The HITECH Act substantially increased the penalties for non-compliance with the HIPAA Privacy and Security Rules. Enforcement began on November 30, 2009, and includes compliance audits and complaint investigations.

There are five Technical Safeguard Standards:

- Access control.
- Audit controls.
- Integrity.
- Person or entity authentication.
- Transmission security.

Technical Safeguards are "the technology and the policies and procedures for its use that protect electronic protected health information and control access to it."[4] The Technical Safeguard Standards protect a dental practice's electronic information assets, including electronic protected health information that is used, disclosed, transmitted, or stored in the practice's "electronic environment." The electronic environment includes all computer workstations, laptops, handheld devices, database servers, applications servers, data management systems, and other electronic devices used in or outside of your practice.[5] Whereas the Administrative and Physical Safeguards that are discussed in Chapters 4 and 6 of this book apply to actions that workforce members in a

[3] 45 CFR 164.304

[4] 68 *Federal Register* 8376.

[5] Increasingly, portable and mobile electronic devices are used as business tools in the health care industry, which increases the risk of a privacy or security breach of electronic protected health information in the absence of appropriate security safeguards. These devices include: "laptops; home-based personal computers; PDAs and Smart Phones; hotel, library or other public workstations and Wireless Access Points (WAPs); USB Flash Drives and Memory Cards; floppy disks; CDs; DVDs; backup media; Email; Smart Cards; and Remote Access Devices (including security hardware)." See the Centers for Medicare & Medicaid Services (CMS) document: "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information," which is included in this book as Appendix 5-1, and is available online at: *http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806rev.pdf.*

dental practice perform routinely or on a daily basis, the Technical Safeguards apply to actions that are related to hardware and software security features and performance.

There are ten Implementation Specifications for the Technical Safeguard Standards. Implementation Specifications are designated by HIPAA as being either *required* or as being *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.

In our examination of the tenth Implementation Specification, encryption, we also will discuss the *Guidance*[6] for securing PHI that HHS released in connection with the HHS Breach Notification Rule. The *Guidance* is discussed in detail in Chapter 1. Practices that secure PHI in compliance with the *Guidance* are unlikely to be required to send notification in the event of a breach.

Fundamentals About Technical Safeguards

Just as you lock doors to protect your physical assets, you also need to lock electronic doors to protect your technology assets. Technical Safeguards are used to protect the *confidentiality*, *integrity*, and *availability* of your dental practice's electronic protected health information. Remember, the Security Rule applies to *electronic* protected health information.

Confidentiality, integrity, and availability are the fundamental properties that underpin privacy and security under HIPAA:

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

As your dental practice develops and implements policies and procedures to fulfill the requirements of the Technical Safeguard Standards, remember to keep these properties of *confidentiality*, *integrity*, and *availability* — C I A — in the forefront of your practice's decision-making. These are important properties to discuss with your Business Associates as well.

[6] *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,* published in the *Federal Register* on August 24, 2009, as part of the Interim Final Rule on 'Breach Notification.' Department of Health and Human Services, Office of the Secretary, "45 CFR Parts 160 and 164: Breach Notification for Unsecured Protected Health Information; Interim Final Rule," *Federal Register*, v.74, n.162, Monday, August 24, 2009, pp.42739-42770.

In dentistry, we increasingly store and move information around electronically, sometimes without giving much thought to its value and the risks involved. The HIPAA Security Technical Safeguards provide a framework to help protect your electronic information and technology assets, especially the electronic protected health information that your practice uses, discloses, transmits, or stores in an electronic environment. Because of the August 24, 2009, Interim Final Rule on *Breach Notification for Unsecured Protected Health Information*, which we discussed in Chapter 1, your dental practice now has decisions to make regarding how to protect the value of your information and technology assets and protect your practice from the consequences of a breach of unsecured PHI.

The HIPAA Security Technical Safeguards apply to **all** electronic media, including computer workstations, laptops, tablets, personal data assistants (PDAs), database servers, application servers, data management systems, and other electronic devices that are used in your practice or that are used outside of your practice (such as a Web hosting server).[7]

The Security Rule requires that access to systems containing electronic protected health information be on a "need to know" basis—with the goal of restricting access to protected health information to workforce members with the appropriate business functions and need. There are numerous methods to enforce access control, such as by operating system, application, individual user identification through password or biometric entry, role within organization, membership within a particular group, encryption, or other control means, such as those related to time or physical location.

As we mentioned in Chapter 4 in the discussion on Administrative Safeguards, 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.[8]

We recommend that you download and read this document. We will refer to this document in the discussion that follows. For each of the Technical Security Standards, we provide in a footnote a specific reference in Appendix 5-2 to the "Technical Safeguards" page or pages in NIST Special Publication 800-66 Revision 1 that refer to that Standard. For example, NIST pages 40-41 outline and describe activities and sample questions that your dental practice should consider in addressing the Implementation Specifications for the first Standard discussed: Access Control, as shown in Table 5.1.

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

Finally, you are not alone when it comes to complying with the Technical Standards for safeguarding electronic protected health information. Ask your software and hardware vendors for help. If you need consulting expertise, start by asking other dentists with practices similar in size to yours which consultants they use.

[7] See Appendix 5-1: "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information."

[8] 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 5-2 includes information from this document relating to the technical Standards and their Implementation Specifications.

Table 5.1 Technical Safeguard Standards at a Glance

Security Standard	Implementation Specification	Required or Addressable
Access Control	Unique User Identification	Required
	Emergency Access Procedure	Required
	Automatic Log-off	Addressable
	Encryption and Decryption	Addressable
Audit Controls		Required
Integrity	Mechanism to Authenticate Electronic Protected Health Information	Addressable
Person or Entity Authentication		Required
Transmission Security	Integrity Controls	Addressable
	Encryption	Addressable

ADA TIP

Remember, in reviewing the following security Safeguard Standards and their Implementation Specifications, you "may use any security measures that allow [your dental practice] to reasonably and appropriately implement the Standards and Implementation Specifications."[9] *Reasonable* and *appropriate* measures should not interfere with delivery of care to your patients or obtaining payment for services rendered. "In deciding which security measures to use, [your dental practice] must take into account the following factors:

- The size, complexity, and capabilities of [your dental practice].
- [Your dental practice's] technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to electronic protected health information.[10]

[9] 45 CFR 164.306(b)(1).
[10] 45 CFR 164.306(b)(2).

Standard: ACCESS CONTROL

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR[11] Part	Implementation Specification	Required or Addressable
Access Control	68 FR 8378 45 CFR 164.312(a)(1)	i. User Identification ii. Emergency Access Procedure iii. Automatic Logoff iv. Encryption and Decryption	Required Required Addressable Addressable

What is Required: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in the Administrative Safeguard Standard "Information Access Management" (see Chapter 4, pp.16-17).[12]

What This Standard Means for Your Dental Practice:

This Safeguard Standard requires your dental practice to establish policies and procedures that govern how your electronic information systems will allow authorized persons or automated processes (like backup routines, system updates, etc.) to have access to electronic protected health information.

Your dental practice will need certain software features to achieve access control. These features may be part of the software application, the computer's operating system, the database management system, or a combination thereof.

There are four approaches to controlling who has access, when they may have access, and where they may have access to information. Your dental practice will have to determine which approach is most appropriate, as determined in your risk analysis. The four approaches are:

Access Control List: The dental practice manager authorizes various workforce members to have access to the specific applications and databases that they need to do their jobs.

User-Based Access Control: The dental practice manager authorizes various workforce members to have access based on user identity (e.g., dentist, office manager, etc).

Role-Based Access Control: The dental practice manager authorizes workforce members to have access based on their job functions.

Context-Based Access Control: The dental practice manager authorizes workforce members to have access based on job function, but with restrictions, such as access only during specific hours or on certain days, or at specific workstations.

[11] *Code of Federal Regulations*
[12] Also see Appendix 5-2, *Access Control*, NIST pp.40-41.

Sample Policy

Our dental practice will implement technical policies and procedures for electronic information systems that maintain electronic protected health information, allowing access only to those persons, entities, or automated processes (e.g., software programs) that have been granted access rights as specified in the Administrative Safeguard Standard "Information Access Management" (see Chapter 4, p.16).

Sample Procedures

Our dental practice will establish policies and procedures to show how our electronic information systems allow access to electronic protected health information, to whom (or what), and for what purposes. We will do this by using access control features in our software applications, operating system, database management system, or some combination thereof, and by documenting in writing what we have done. Our practice's risk analysis will determine how we will control access by list, user identity, role, or context.

ADA TIP

Make sure that your practice's Security Official reviews workforce member access on a regular basis. This should include a review of automated processes such as remote backup, integrity checks, or other authorized activities. When reviewing automated processes, determine whether HIPAA privacy requires patient authorization for the disclosure of protected health information, and which disclosures can be made without authorization for purposes of treatment, payment, and health care operations.

Implementation Specification: Unique User Identification

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Access Control	68 FR 8378 45 CFR 164.312(a)(2)(i)	i. Unique User Identification	Required

What is Required: Assign a unique name and/or number for identifying and tracking user identity.

Sample Policy

Our Security Official will determine each workforce member's need for access to electronic protected health information, and make sure that workforce members only have access to the information that is necessary to perform their work responsibilities. Our practice will identify users and track user identity through assigned unique names and/or numbers. Our dental practice prohibits any workforce member from sharing or otherwise disclosing his or her username, number, or password to other workforce members. Our dental practice prohibits the use of generic or shared user ID credentials to access records containing electronic protected health information.

Sample Procedures

Our Security Official is responsible for assigning a unique user ID to each workforce member in our dental practice. In addition, our Security Official is responsible for:

- Assigning, managing, and tracking user ID credentials in our dental practice.[13]
- Defining and enforcing our practice's policy on sharing and disclosing user ID credentials.
- Instructing users that initial assigned passwords must be changed to user-selected passwords on initial login.
- Requiring users to change their passwords every <30>, <60>, or <90> days, as determined appropriate through the practice's risk analysis.

ADA® TIP

Each workforce member in the dental practice should provide his or her current password in a sealed envelope to the practice's Security Official for storage in a secure location in order to provide system access in an emergency.

Implementation Specification: Emergency Access Procedure

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Access Control	68 FR 8378 45 CFR 164.312(a)(2)(ii)	ii. Emergency Access Procedure	Required

What is Required: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Sample Policy

Our Security Official will establish methods of emergency access to electronic protected health information in the event of loss of data and systems due to an emergency or disaster such as fire, earthquake, flood, tornado, hurricane, vandalism, terrorism, power outage, or system failure.

Sample Procedures

Our Security Official will identify, as part of our practice's risk analysis, the types of emergencies and disasters that could impair our practice's ability to access our patients' electronic protected health information. Our practice realizes that a delay in accessing our patients' electronic protected health information could hinder our ability to provide appropriate treatment and possibly pose a risk to the patient's health.

[13] In a small dental practice, unique user access is often based on a workforce member's identity. In a larger practice, unique user access may be based on the job responsibilities of each workforce member.

The Security Official will work with our practice's electronic system vendors to establish and test emergency access procedures to accommodate the types of emergencies and disasters that our practice identified in its risk analysis.

Our Security Official will train authorized workforce members on how to implement and periodically test those procedures.

Our Security Official will document emergency access procedures and distribute instructions for initiating emergency access procedures to designated authorized workforce members. As one of those procedures, the Security Official may establish, in consultation with the practice's electronic system vendors, a special user password that would allow the Security Official and at least one designated authorized backup workforce member full access to electronic protected health information in an emergency or disaster situation. In such a situation, the Security Official would be responsible for documenting in a special emergency access log[14] the actions taken and by whom. The special emergency access log should include any incidence of abuse of emergency access and the sanctions imposed on the individuals responsible.

ADA TIP

The security official and at least one designated authorized workforce member should have emergency access to all electronic protected health information. Ask your electronic system vendor to develop a unique password for emergency access.

Implementation Specification: Automatic Logoff

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Access Control	68 FR 8378 45 CFR 164.312(a)(2)(iii)	iii. Automatic Logoff	Addressable

What to Do:[15] Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Sample Policy

Our Security Official will ensure that automatic logoff procedures are in place on all systems and devices that provide access to electronic protected health information in our dental practice.

[14] See Appendix 5-3 for sample form: *Emergency Access Log.* Along with a special user password procedure for emergency or disaster situations, larger practices should implement a trigger mechanism that alerts appropriate management personnel that emergency procedures are underway.

[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.

Sample Procedures

Our Security Official will establish an inventory of all of the practice's systems and devices that provide access to electronic protected health information. Our Security Official will check each system and device that accesses or stores electronic protected health information to make sure its screen-saver locks are enabled and set to 10 minutes or less.[16] An authorized user of any such system or device must use his or her username and password to unlock a locked system or device. The Security Official will enforce the automatic logoff procedure and sanction any workforce member that adjusts a locking interval. The Security Official will ensure that workforce members are trained to lock any electronic systems or devices located in patient service areas while a patient is in the area.

ADA® TIP

The Security Official should regularly remind all workforce members not to leave a patient unattended near a system or device that has not been logged off.

Implementation Specification: Encryption and Decryption

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Access Control	68 FR 8378 45 CFR 164.312(a)(2)(iv)	iv. Encryption and Decryption	Addressable

What to Do:[17] Implement a mechanism to encrypt and decrypt electronic protected health information.[18]

Sample Policy

Our Security Official is responsible for safeguarding our practice's electronic protected health information. Our practice's *Notice of Privacy Practices* outlines our practice's policy on communication over *open* networks or electronic systems. Our policy is to inform patients by e-mail that an electronic message from the practice can be accessed on the practice's server only when the patient provides a unique patient ID and password for access. In conformance with the *Guidance* in the HHS Breach Notification Rule[19], our dental practice as a matter of policy encrypts **all** electronic protected health information *at rest* in the practice's database and *in motion* through outbound communications using the technologies and methodologies specified in the *Guidance*.

[16] Lockout times for small dental practices should be 5 minutes or less in high traffic areas, and 10 minutes or less in limited access areas. Lockout times for large dental practices should be 2 minutes in high traffic areas, but 10 minutes or less in limited access areas. Irrespective of size, the timing of lockout intervals for particular systems and devices should be an outcome of the dental practice's risk analysis.

[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] Encryption converts a message in a file or document from a readable to an unreadable state. Decryption is the reverse process: it allows encrypted information to be converted into a readable state.

[19] 'Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals' of the August 24, 2009, Interim Final Rule: *Breach Notification for Unsecured Protected Health Information*, 74 *Federal Register* 42742-42743.

Sample Procedures[20]

The Security Official will ensure that all electronic protected health information *at rest* or *in motion* is encrypted, and thus secure, as outlined in the *Guidance* referenced in our policy on this matter. As necessary, the Security Official will work with the Privacy Official to update the practice's *Notice of Privacy Practices* to reflect this policy, to indicate that the practice will not send to its patients unencrypted e-mail containing electronic protected health information, and that patients wishing to communicate by e-mail with the practice will be required to use a secure e-mail application to retrieve any such information.

ADA TIP

Even though this Implementation Specification is addressable, we strongly recommend that your practice encrypt electronic protected health information at rest and in motion, thereby 'securing' such information and making it 'unusable, unreadable or indecipherable to unauthorized individuals.'

Standard: AUDIT CONTROLS

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Audit Controls	68 FR 8378 45 CFR 164.312(b)		Required

What is Required: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.[21]

What This Standard Means for Your Dental Practice:

Small and large dental practices are required to have in place audit controls to monitor (record and examine) activity on their electronic systems. They also must monitor and regularly review audit records to ensure that all activity is appropriate. Monitoring and review should include logons and logoffs, file accesses, updates, edits, other system activity, and security incidents. Audit trail reviews can be time consuming and tedious, but should be done as close as possible to real time. An audit trail review does your practice little good if you learn that your system experienced an unauthorized access a month earlier. Failure to comply with this Standard may be evidence that your practice was capable of discovering an unauthorized access, but that it neglected to audit and take corrective action.

[20] If your practice does not communicate electronically over an open network, you may not need to implement this specification, which is addressable. If this is the case, be sure to document your decision, and explain why this specification does not apply to your practice. Be advised, however, that the Breach Notification Rule reference in the Sample Policy also covers *data at rest* in your practice's servers. If those data are 'unsecured' and a breach occurs (e.g., you have a break-in and workstations or servers are stolen), your practice will be responsible for notifying your affected patients that their electronic protected health information may have been or has been breached (you must also notify HHS and, in some cases, the media). You must address the risk of a potential breach in your practice's risk analysis, and we recommend that you balance the cost of encryption against the potential expected cost of complying with breach notification requirements. The interim breach notification requirements were effective September 23, 2009, and enforcement and sanctions for non-compliance are effective February 22, 2010, for breaches discovered on or after that date.

[21] Also see Appendix 5-2, *Audit Controls*, NIST pp.42-43.

Sample Policy

Our Security Official will train workforce members to comply with the practice's technical safeguards regarding the use of electronic systems and access to and protection of electronic protected health information, and enforce workforce compliance through sanctions. Our Security Official will review system-generated audit logs regularly, as frequently as the practice's risk analysis deemed necessary, and will initiate appropriate actions to correct accessibility issues or incidents and to sanction inappropriate use, as necessary. The Security Official will confirm and document that existing and newly acquired software has auditing capabilities and that such capabilities are enabled.

Sample Procedures

Our Security Official will monitor all systems containing electronic protected health information for unauthorized intrusions. The Security Official will review access logs on a weekly basis to detect unauthorized access attempts. The Security Official will make sure that audit logs are retained in accordance with the Security Rule document retention requirements, and destroyed thereafter. The Security Official will impose appropriate sanctions under the dental practice's sanction policy and procedures on any workforce member found to have attempted or achieved unauthorized access.

ADA® TIP

Regularly reviewing audit logs to detect unauthorized access attempts, in combination with an effective sanction policy, will reduce the likelihood of a security incident. Audit logs may be kept in an electronic format, but they must remain *accessible* to authorized users. Audit logs must be retained for six years after the last dated entry.

Standard: INTEGRITY

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Integrity	68 FR 8378 45 CFR 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	Addressable

What is Required: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.[22]

What This Standard Means for Your Dental Practice:

Along with confidentiality and availability, integrity is one of the three key components of a successful security strategy that safeguards your dental practice's electronic systems and electronic protected health information. Integrity means that your dental practice's data are dependable and accurate. It means that your practice's data are not altered or destroyed in an inappropriate manner. Inaccurate or missing data could result in harm or even death of a patient.

[22] Also see Appendix 5-2, *Integrity*, NIST pp.44-45.

Data can become inaccurate or corrupt for a number of reasons: data entry errors, hacking, tampering, storage device mechanical errors, transmission errors, or faulty integration of data elements or records from downloaded reports, say, from a lab. Software or programming bugs, computer viruses, and human error also can corrupt data records. It is imperative that your practice protect its data from unauthorized alteration and destruction, and that your practice knows if its electronic protected health information has been inappropriately altered or destroyed.

ADA TIP

Protecting data integrity is one of the fundamental components of a successful security strategy that safeguards your dental practice's electronic systems and electronic protected health information.

Implementation Specification: Mechanism to Authenticate Electronic Protected Health Information

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Integrity	68 FR 8379 45 CFR 164.312(c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Addressable

What to Do:[23] Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Sample Policy

Our Security Official is responsible for implementing mechanisms for corroborating the integrity of electronic protected health information.

Sample Procedures

Our Security Official shall:

- Work with our dental practice's information system vendor to understand how our system achieves and checks data integrity, how intrusions are detected, and how integrity performance is measured and reported.
- Ensure that users of our dental practice's electronic systems authenticate their access to those systems and electronic protected health information therein.
- Ensure that our practice's electronic systems have intrusion detection that provides audit trails and alerts of potential hacking.
- Test our electronic systems and their backup counterparts every < > days to identify any mechanical errors.

[23] 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.

- Confirm that data transmitted via standard network protocols is the same as data received.
- Every < > days, test and monitor the results of data integrity checks on applications, databases, operating systems, networks, servers, workstations, and backup storage devices.

ADA® TIP

Regularly testing the integrity of your dental practice's electronic systems and electronic protected health information therein is a key component of a successful security strategy. Your vendor may perform this for you as a part of your service agreement, but it is necessary to verify this and document it appropriately.

Standard: PERSON OR ENTITY AUTHENTICATION

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Person or Entity Authentication	68 FR 8379 45 CFR 164.312(d)		Required

What is Required: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. The Implementation Specification instructions are contained in the language of the Standard and thus required.[24]

What This Standard Means for Your Dental Practice:

This Safeguard Standard requires your dental practice to implement procedures that authenticate[25] any person or entity that seeks access to your electronic systems and electronic protected health information contained therein. As such, it requires more than just providing authentication credentials for user access; it requires that you maintain and monitor audit trails so that your practice can authenticate a person or entity that is reading, altering, and transmitting electronic protected health information, or attempting to do so.

Sample Policy

Our Security Official has implemented a policy that any user seeking access to our dental practice's electronic systems and electronic protected health information shall possess credentials that authenticate access. Credentials entered by a potential user must match those stored in the electronic system in order to gain access.

[24] Also see Appendix 5-2, *Person or Entity Authentication*, NIST p. 46.

[25] Authentication is a round trip process: Computer asks, 'Who Are You?' and awaits response. Following response, computer tells potential user to 'Prove It' and potential user provides positive identification in order to gain access. Such identification could be something user knows (user ID, name, security question, personal ID number, password phrase); something user carries (ATM card, token, swipe card, badge); something that is part of user (biometric, such as finger image, voice scan, iris or retina scan).

Sample Procedures

Our Security Official shall define technical and procedural mechanisms to authenticate the identity of users and/or processes that access our electronic systems and electronic protected health information, and shall implement procedures to monitor and enforce authentication. Such mechanisms will be a combination of authentication credentials and audit trails to enforce authorized access. Our Security Official shall ensure that electronic system users authenticate themselves with credentials, such as a combination of username and password or a biometric authentication such as thumbprint or retina scan.[26] Our Security Official permits users to synchronize usernames and passwords on multiple electronic devices that are owned by the practice, provided the password is strong, appropriate security safeguards are in place, and data are encrypted on the electronic devices.

ADA TIP

A combination of authentication credentials and audit trails helps to ensure authorized access to your dental practice's electronic systems and electronic protected health information. Authentication can work together with encryption and decryption to protect confidentiality.

Standard: TRANSMISSION SECURITY

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Transmission Security	68 FR 8379 45 CFR 164.312(e)(1)	i. Integrity Controls ii. Encryption	Addressable Addressable

What is Required: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.[27]

What This Standard Means for Your Dental Practice:

This Safeguard Standard requires your dental practice to implement a system that protects electronic protected health information while it is being transmitted outside of your practice. You may have a local network with no connectivity to any entity outside of your office, but in today's electronic environment this is increasingly rare. Your IT vendors likely have some connection to your network so that they can provide your practice with timely IT support, data backup, application backup, integrity checks, system updates, and enhancements. Most dental practices also have Internet access, so a poorly designed network can threaten your electronic systems, especially if it compromises the *availability* and *integrity* of your practice's data.

[26] For an excellent discussion and useful guidance on password management, see Karen Scarfone and Murugiah Souppaya, Guide to Enterprise Password Management (Draft), NIST Special Publication 800-118 (Draft), April 2009, which is available online from the National Institute of Standards and Technology (NIST) at: *http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf*.

[27] Also see Appendix 5-2, *Transmission Security*, NIST p. 47.

Today's systems are more secure, but older systems — especially operating systems that are not regularly updated — likely contain unused, unnecessary, or obsolete programs that leave your practice exposed on open networks. Ask your IT vendor or consultant to help you identify systems that you can discard, and those that can be updated and still be useful to the practice. You may want to consider asking your IT vendor or consultant for help in auditing your existing system security and for "hardening" any existing systems to enhance your practice's security. Before installing any fixes or patches, evaluate them first in a test environment. If you install fixes or patches without first evaluating them in a test environment, you risk losing critical business data and you risk impairing the quality of, and access to, electronic protected health information on your servers or network devices.

The growing use of wireless networks is one of the biggest threats to network security. Wireless technology allows computer workstations, laptop, tablet, and notebook computers, and portable handheld devices such as portable data assistants (PDAs) equipped with wireless access modems to connect to a local area network (LAN) without having to connect the device via cable. Mobile telephones with photo capabilities also create privacy and security challenges. Wireless devices and LANs must be included in your dental practice's security and privacy strategies if you use them. If you have a wireless network, it *must* be secured.

In addition to advances in technology, which enhance convenience and raise security issues at the same time, the potentially onerous and costly HITECH Act provisions on breach notification require dental practices to consider in their risk analyses how they will address data security in the context of this Standard. We shall address this further in the discussion pertaining to this Standard's second Implementation Specification: Encryption.

ADA TIP

In a business environment that will be increasingly interoperable, with electronic information moving between your practice and other Covered Entities and Business Associates, your practice must regularly address potential threats and vulnerabilities to the movement of that information.

Implementation Specification: Integrity Controls

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Transmission Security	68 FR 8379 45 CFR 164.312(e)(2)(i)	i. Integrity Controls	Addressable

What to Do:[28] Implement security measures to ensure that electronically transmitted protected health information is not improperly modified without detection until disposed of.

Sample Policy

Our Security Official is responsible for implementing a policy that will ensure that electronic protected health information has not been altered without appropriate knowledge and approval of our dental practice.

Sample Procedures

Our Security Official shall assign unique user username/password combinations to persons authorized to log onto our dental practice's electronic systems. Our Security Official shall ensure that all entries into our electronic systems are tracked appropriately by audit trail technology. Our Security Official shall regularly review audit trail reports and identify any unauthorized changes to electronic protected health information. Our Security Official shall immediately notify any person, and that person's supervisor, who is observed or recorded making unauthorized changes to electronic protected health information, and shall apply appropriate sanctions for such unauthorized changes. In addition, our Security Official will work with our technology vendors to ensure that our system runs routine integrity checks and alerts the Security Official and practice ownership to any problems detected.

ADA® TIP

An authenticated user of our dental practice's electronic systems is subject to disciplinary sanctions, up to and including termination, for making unauthorized changes to our practice's electronic protected health information. Integrity problems generated by the system itself need to be investigated promptly and causes determined. Consultation with the system vendor, or, in some cases, a disinterested and fully qualified third party, may be necessary.

[28] 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.

Implementation Specification: Encryption

Technical Safeguard Standard	Federal Register (FR)/ 45 CFR Part	Implementation Specification	Required or Addressable
Transmission Security	68 FR 8379 45 CFR 164.312(e)(2)(ii)	ii. Encryption	Addressable

What to Do:[29] Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Sample Policy

As a matter of policy, our dental practice encrypts **all** electronic protected health information at rest in the practice's database and in motion through outbound communications in conformance with the technologies and methodologies specified in the 'Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals'[30] of the August 24, 2009, Interim Final Rule: *Breach Notification for Unsecured Protected Health Information*.

Sample Procedures[31]

The Security Official of our dental practice will ensure that all electronic protected health information *at rest* or *in motion* is encrypted, and thus secure, as outlined in the *Guidance* referenced in our policy on this matter. The Security Official will ensure that this policy is reflected accurately in an update of our *Notice of Privacy Practices*. In addition, the Security Official shall make sure that the *Notice of Privacy Practices* indicates that we will not send our patients unencrypted e-mail containing electronic protected health information. Rather, patients wishing to communicate by e-mail with the practice will be required to have a unique username and password, and login to the practice's secured website to send or retrieve any such information.

NOTE: Many practices do not have websites with secured e-mail functions, so they may wish to avoid exchanging e-mails that contain electronic protected health information without encryption. They also may consider enlisting a Business Associate to provide a secured e-mail service under the terms of a Business Associate Agreement.

ADA TIP

Even though this Implementation Specification is addressable, we strongly recommend that your practice encrypt electronic protected health information at rest and in motion, thereby 'securing' such information and making it 'unusable, unreadable or indecipherable to unauthorized individuals.'

[29] 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.

[30] 74 *Federal Register* 42742-42743.

[31] If your practice does not communicate electronically over an open network, you may not need to implement this specification of the Standard, which is addressable. If this is the case, be sure to document your decision and explain why this specification does not apply to your practice. Be advised, however, that the Interim Final Rule referenced in the Sample Policy covers *data at rest* in your practice's servers. If those data are 'unsecured' and a breach occurs, your practice will be responsible for notifying your affected patients that their electronic protected health information may have been or has been breached. You must also notify HHS and, in some cases, media outlets of a breach of unsecured PHI. You must address the risk of a potential breach in your practice's risk analysis, and we recommend that you balance the cost of encryption against the potential expected cost of complying with breach notification requirements. The breach notification requirements are effective September 23, 2009, and enforcement and sanctions for non-compliance are effective February 22, 2010, for breaches discovered on or after that date.

Chapter Summary

Technical Safeguards are defined as "the technology and the policies and procedures for its use that protect electronic protected health information and control access to it."[32]

Most of us move information around without giving much thought to its value, or to the consequences if the data are altered or lost. The Technical Safeguards component of the HIPAA Security Rule provides five security requirements that will help protect your dental practice's information technology assets, including electronic protected health information that your practice uses, discloses, transmits, or maintains at rest in a storage device.

The HIPAA Security Rule requires that access to your electronic systems containing electronic protected health information be on a "need to know" basis in your business environment, with the goal being that only persons with the appropriate business functions and credentials are able to access such information. There are numerous methods to enforce access control, such as by operating system; by application; by individual user identification; by role within an organization; by membership within a particular group; by encryption; by factors such as time or physical location; or some combination thereof.

Enactment of HITECH Act breach notification requirements, as part of the American Recovery and Reinvestment Act signed by President Obama on February 17, 2009, increases the importance of appropriately encrypting your electronic protected health information at rest and in motion in order to make it "secure", thereby eliminating the need for potentially costly notification requirements in the event of a breach of such information. Doing so will strengthen the availability, confidentiality, and integrity components that are fundamental to your dental practice's achieving its security objectives and minimizing threats and vulnerabilities to that information.

ADA® TIP

1. Encrypt your practice's electronic protected health information at rest and in motion.
2. Implement unique user identification if you have not done so already.
3. Employ some method of authenticating the identity of users and processes that access electronic protected health information. There are a number of methods that can achieve this, including the combination of username/password.
4. Check your data integrity regularly by auditing frequently your system access and file edit logs. If you don't have audit trail capability on your existing system, it is time to upgrade now. If the cost of upgrading your system is prohibitive, consider the costs to your business of file corruption or unauthorized access of electronic protected health information by a bad actor.
5. System access and file edit logs may be stored in electronic media, but must remain accessible according to HIPAA documentation Standards.
6. Don't send e-mails with electronic protected health information over open networks. Use encryption, or, when possible, a secured web e-mail service maintained in your office or by a Business Associate.

[32] 68 *Federal Reserve* 8376