the Journal of CONTEMPORARY DENTAL PRACTICE at www.thejcdp.com
Volume 5 Number 3 August 15, 2004 Summer Issue

The Health Insurance Portability & Accountability Act and the Practice of Dentistry in the United States: System Security

Joseph E. Chasteen, DDS, MA; Gretchen Murphy, MA;
Arden Forrey, PhD; David Heid, DDS

Abstract

This article reviews the issues related to the Health Insurance Portability & Accountability Act (HIPAA) security rule that apply to dental practice. The security rule specifically addresses individually identifiable health information that is transmitted or maintained in electronic media. System security must be applied to the entire technical infrastructure for the practice environment as well as to the work culture on a daily basis and must be thought of as an enterprise asset. Security refers to all of the policies, procedures, tools, and techniques used to assure that privacy and confidentiality are adequately addressed in a healthcare system. HIPAA requires all covered entities that transmit or maintain electronic health information perform, and document, a risk assessment for security and develop a security plan to address major areas of concern. A self-assessment tool is provided in this article.

Keywords: HIPAA, Electronic Protected Health Information (EPHI), electronic health record, dental practice, computer, system security

Citation: Chasteen JE , Murphy G, Forrey A, Heid D. The Health Insurance Portability & Accountability Act and the Practice of Dentistry in the United States: System Security. J Contemp Dent Pract 2004 August;(5)3:158-167.

Introduction

In its quest to foster the use of electronic health record keeping and the use of electronic transmission of claims to third party payers, the United States government recognized the vulnerability of sensitive health information about an individual to potential abuse, unauthorized distribution, and exploitation. It also recognized the vulnerability of such health data to loss due as a result of computer malfunction and catastrophic events such as fire, storms, earthquakes, and floods to mention a few. As a result, the 1996 Health Insurance Portability & Accountability Act (HIPAA) section on Administrative Simplification addressed the use and protection of the confidential health information about a patient in an emerging electronic care documentation environment. The security rule specifically addresses individually identifiable health information that is transmitted or maintained in electronic media. This means the dental practice must base their security requirements initially on the security provisions contained within the Privacy Rule portion of the legislation and then adopt the specific Security Rule requirements for Electronic Protected Health Information (EPHI) discussed in this article.

While HIPAA is somewhat complicated, it basically consists of three key sets of rules. These rules include those relating to patient privacy, the electronic transmission of transaction codes between parties, and the security of patient care data.

Previous articles have probed the Electronic Oral Health Record (EOHR) and the associated privacy and administrative transaction issues within the HIPAA context.[1-3] This paper will examine the system security issues for the dental practice information architecture, beginning with the requirements of the recently released (February 20, 2003) HIPAA security regulations.[4]

System security must be applied to the entire technical infrastructure for the practice environment and must be thought of as an enterprise asset. Although technologic infrastructure is likely to continually change rapidly, it can be separated from global business conceptual content to preserve essential business functionality. These global issues will be addressed in this context.

System Security

Privacy refers to the right of the individual to keep their protected health information private and to control who may access it.[2] Confidentiality refers to the responsibility of the healthcare workforce to maintain the individual patient's private information so it is NOT disclosed inappropriately. Security refers to all of the policies, procedures, tools, and techniques used to assure privacy and confidentiality are adequately addressed in a healthcare system. HIPAA requires all covered entities that transmit or maintain electronic health information perform, and document, a risk assessment for security and develop a security plan to address major areas of concern. Security rules are divided into four categories:

- Administrative Procedures
- Physical Safeguards
- Technical Security
- Network and Communication Security

Administrative Procedures

These procedures provide for policies and procedures to guard data integrity, confidentiality, and availability. They are the formal documentation of security for the organization's health information. The HIPAA rule calls for a certification from each healthcare organization or dental practice that states appropriate security has been implemented. A security audit can be performed internally. The administrative policies and procedures provide formal documentation of the following:

- The conduct of a security audit and analysis of potential risks and vulnerabilities to potential breaches of the security of protected health information. This is the basis for developing the basic security program for institutions and practices.
- Implementation of security measures sufficient to reduce risks to a reasonable and appropriate level. These would be contained within the practice policies and procedures.
- Establishment of sanctions for workforce members who fail to comply with the established security policies.

- Establishment of policies to regularly review system activity in order to detect potential breaches.
- Identification of a specific individual assigned as security officer to oversee security measures are used and that personnel protect data in their routine activities. This individual also is responsible for tracking security incidents and providing security training for employees.
- Creation of access controls based on a formal access authorization process that designates how access is established. The process has to also address how access can be modified and used with appropriate authentication methods and with specified use of audits.
- Formulation of contingency plans that include applications and their data criticality, a data backup and data recovery plan, as well as the use of chain of trust agreements for the electronic exchange of data.
- The formal protocols for processing patient records.
- Identification of authorization control mechanisms to monitor use and disclosure of health information, and mechanisms for transmission of records. Patient signed authorizations for disclosure procedures are included here.
- Management of the security configuration to include: documentation, hardware/software installation, maintenance review, testing for security features (including Virus Testing), and a hardware/software inventory.
- The plan for personnel security to assure supervision, maintenance of access authorization, personnel clearance, and training.
- Establishment of security training requirements.

The detail in several of these aforementioned evaluation items is further defined in the discussion of physical and technical safeguards.

Physical Safeguards

Safeguards can be organized by media, physical controls, and workstation use. Media control policies are needed to govern the receipt and removal of hardware/software (i.e., diskettes, tapes, optical disks). They spell out who is authorized to set up or add software to workstations, how accountability for these activities is tracked, and details on data backup, storage, and disposal of patient data.

Physical controls are based on formal, documented policies and procedures for limiting physical access while ensuring properly authorized access is allowed. Access controls are tied to user roles or functions to conform to key elements of the privacy rule. Physical control policies and procedures cover equipment control, facility security plans, testing, maintenance records, and verification of authorization prior to physical access. For example, a sign-in process for on-site visitors is included. Keep in mind access is keyed to a user ID, authentication protocols, and need-to-know procedures for personnel access.

Workstation use policies and procedures describe appropriate workstation functions and how they should be performed (i.e., logging off before leaving a terminal unattended). Secure workstation location policies help limit unauthorized viewing of monitor screen displays. Often this means simply positioning the screen so visitors are unable to see it. Physical controls for locking individual workstations and computer installation sites need to be designated.

Office level security procedure is also included here. This addresses how patient records are physically maintained and protected from unauthorized access.[4]

Technical Security

Technical security is the aggregation of technical capabilities used to safeguard data integrity, confidentiality, and availability and is based on access control. Access control is determined by one of three methods:

- Context-based (scenario) access
- Role-based (healthcare team member responsibility) access
- User-based (business need to know) access

These are alternatives for healthcare organizations to use. They enable institutions to set up a formal, accountable process by which individuals are granted authorization rights to access protected health information. Emergency access must be a defined option with all three alternatives.

Once the access authorization method is selected, the technical mechanisms follow. Technical user authentication (User ID) methods are required to employ unique user identification. Such tools as biometrics (e.g., fingerprint, iris of the eye), passwords, personal identification number (PIN), telephone callback, or tokens (e.g., card swiped at the workstation) are used in multiple ways in the banking and business community and are well established options for healthcare.

Consider the following role-based access scenario. Individuals who have been authenticated by their role in the practice, or organization can be appropriately authorized to access pre-identified levels of protected health information. Once they have signed on to a software application, the system automatically checks their user ID against a "role based" authorization table. Their role determines the approved access to the patient information they need to perform their job. A required automatic audit mechanism then tracks employee access and records any actions taken on data. If the individual seeks access to unauthorized data, the audit mechanism records the attempt.

Not only do audit controls identify suspect data access actions, they also provide aggregate data so institutions can respond to potential security weaknesses. Audit tools typically include at a minimum: user name and identification, patient name, type of data accessed, and date the information is accessed. Effective audit reports focus on patterns of access as well as individual cases.

Finally, if the individual leaves a workstation and fails to exit the system, technical security requires automatic logoffs be in place to limit the exposure of such an unguarded workstation.

Small dental practices can meet the technical requirements for access control, entity authentication, and authorization control by simply assigning a user name and password combination to each authorized employee. The associated policies regarding responsibility for password accountability would be documented in the security policy for the practice.[4]

Network and Communications Security

Healthcare organizations that use communications and networks need to protect health information that is transmitted electronically over open networks. One example of a growing method of exchanging health information over networks is electronic mail. Here, and for other network settings, encryption is required to assure that such communication cannot be easily intercepted and health information is protected from access through external communication points.

Where specific provider organizations use private, secure networks, encryption can be an option. Specifics of the Security Rule for communication and networks state there must be integrity controls and message authentication at a minimum. Either access controls, previously discussed, or encryption is required. Entity authentication (verifying the source and their access rights), alarms, audit trails, and event reporting must be employed when healthcare organizations use networks for communications.[4]

The HIPAA Security Rule provides for a uniform level of protection of all health information that is stored or transmitted electronically and is

identifiable to an individual. The standard applies not only to the transactions adopted under HIPAA, but to all individual health information that is accessed, maintained, or transmitted. The dentist should consult the American Dental Association (ADA) Technical Report 1031 on Internet Security for Dental Information Systems[5] with respect to the technical issues that may relate to the practice's information architecture.

While the Security Rule does not currently require the use of an electronic, or digital signature, those who choose to use one when transmitting individually identifiable health information must meet an electronic signature standard imposed by HIPAA in order to ensure message integrity, user authentication, and non-repudiation. Message integrity means the entire original message sent has been received. User authentication means the individual that has been noted to have composed the material is who he/she says he/she is (digital signature). Non-repudiation means the material received and attributed to the authenticated author has been received not only in its entirety but also in an unchanged form that cannot later be claimed as not attributed to that author.

Both encryption and authentication are computational procedures that transform a string of characters into another string by a defined method; authentication produces a checksum that is attached to the string beforehand so the reader can recalculate and compare at a later time to verify the character string has not been changed. This capability will be useful in HIPAA transactions and in the electronic oral health record (EOH) which receives such information as consultations, referrals, or other textual reports from other practitioners.

E-mail transmission of identifiable patient information is not forbidden by HIPAA regulations, but the regulations do require the information be encrypted so it cannot be understood if intercepted. The communication of all uniquely identifiable patient data, including that in the messages of the HIPAA administrative transactions and e-mail, must be protected from outside interception. Encryption is the common technique for ensuring this privacy. A variety of telecommunications methods exist for this purpose and the Suppliers of telecommunication services to the healthcare community are currently working on common conventions (standards) for incorporating these capabilities into the EOHR and practice management products and services for dentists.

The ADA Standards Committee for Dental Informatics (SCDI) will make known the conventions most beneficial to dentists and how to specify these requirements in the procurement of appropriate computer systems for dental practice. Dentists should be aware the requirements in support of HIPAA transactions will have equal applicability to EOHR components of their office practice information architecture even if the present practice architecture doesn't yet contain an EOHR component. This is an information system dimension that is referred to as "interoperability" and should be applicable to data flow between dental and other healthcare specialty practices as dentists become equal partners in healthcare teams in their communities. Thus, this global perspective must be fostered during the current focus on HIPAA administrative transaction capabilities. In short, encryption means when a message has been assembled, the string of characters comprising it is fed to a software component that converts the string mathematically into another string in which all characters have been changed; this string is then fed to those components that transmit it to its designated destination. When it arrives at its destination, a component in that environment uses the accompanying information to convert it back into the original string and present it to the components there that disassemble the transmitted string into the concepts originally taken from the source EOHR or other records and then appropriately file the information sent into the receiving practice's records.

The intent of encryption is to protect electronically transmitted health information so that it cannot be, intercepted or interpreted by parties other than the intended recipient. In addition, the information must be protected from intruders gaining unauthorized access to computer systems. It is recommended if e-mail is used to transmit patient identifiable information then the Centers for Medicare and Medicaid Services (CMS) - formerly Health Care Financing Administration (HCFA) - Internet Security Policy guidelines should

Table 1. Security self-assessment tool for evaluating current practice.

Key Compliance Issues	In Place	Not in Place	Notes
Unique User Identification (individuals or software program)			
• Identification of person using the system including vendors. (authentication) • Identification of what the user allowed to do (authorization)			
Method used to authenticate users.			
• Password • Token • Biometric • IP address • Other – specify			
Process for emergency access to health information			
• Temporary access trigger for user • Tracking of event			
Auditing of activity (Institutional/Vendor features)			
• Monitoring for abnormal activity on system • Random audits to verify appropriate use of system • Reports designed to identify potential problems			
Process for protecting the integrity of information			
• Only authorized individuals are allowed to change information • Only authorized individual are allowed to delete or destroy information			
Contract with Certificate Authority organization (if applicable)			
• Identification of individuals who need *Certificates for Exchange of information between external entities			
Process for timely termination of user access to system			
Process for timely changes in authorizations to access information (e.g. add new staff)			
Security awareness training for all users			
Sanctions for failure to follow organization's policies and procedures			
Software that centrally monitors the organization's security policies and procedures (if applicable)			
Written contracts with business associates and other external entities who have access to protected information			
Real-time security awareness and incident response monitoring			
• Process to respond to security incidents - policies/ procedures • Plan to mitigate harmful effects of incident • Process to document incidents and outcomes			
Analysis demonstrates that the privacy policies of the organization are supported by the security practices and policies			
Procedures for data backup and protection			
Procedures for data recovery if information system is damaged			
Procedures for operating when system is not functioning			
Protection at the workstation level			
• Physical location and screening • Use and reuse of media • Screen protectors • Other – specify			
Procedures for destruction of data			
Firewalls in place to enforce access control policies between networks			
Active content monitoring of material entering the organization's system from the internet			
Software that monitors the system and sets off an alarm and/or countermeasure when someone attempts to gain unauthorized access			
Software that monitors the system and responds when it identifies a traffic pattern that may be an attack (denial of service, scanning)			
Software that protects web applications from threats (stealing organizational assets, accessing protected data, falsifying transactions)			
Software that simulates attacks (to improve system security)			
Encryption tools			
Virtual private network			
Secure web server			

Source: Hanken , MA ; Murphy, GF; Health Information Administration Program, University of Washington.

be used. CMS is the Department of Health and Human Services agency responsible for Medicare and parts of Medicaid. The CMS policy authorizes use of the Internet for transmission of individually identifiable and other sensitive information as long as the following conditions are met:

1. A acceptable method of encryption is used that insures the confidentiality and integrity of the information being transmitted.
2. An authentication/identification procedure exists to verify the identity of the sender and the intended recipient.

Some experts in the HIPAA regulations feel the Department of Heatlh and Human Services (DHHS) has used these specific conditions as a model in making the performance-based determinations for the final HIPAA regulation.

Consider First Steps

The comprehensive details in the security rule can be daunting. The initial step featured in Administrative Procedures focuses on the security risk analysis of the current environment. This is a practical process that will streamline the follow up steps on updating basic policies and procedures in the practice. Updates can be accomplished, and any new policies and procedures can then be addressed as follow-up. By getting started with a security self-assessment, practice staff can map out an overall security program for the practice. In most cases, tools available for dental practices will assist the process. Table 1 is a sample self-assessment tool that may be used in conjunction with staff education and vendor assessment needs. Note the focus is on the electronic protected health information (EHPI) and the EOHR accordingly.

Conclusions

The dentist should conclude meeting the HIPAA security requirements for dental practices can be reasonably achieved by personal attention. Compliance with self-established administrative policies and the favorable configuration of the physical arrangements of the dental office can address almost all of the key security issues. Existing policy and procedure resources can be modified to address results of security assessment processes. Improvements in the technical components of the office information and communication architecture through careful purchasing steps can deal with the remaining issues. Information system purchasing must be based upon a sound understanding of all of the data and functions in the systems that support the dental practice. This understanding should be based upon the published ADA EOHR Standards.

The ADA has announced the availability of a security rule compliance kit by the middle of 2004. The kit is designed to assist dental professionals with the information needed to achieve compliance by the April, 2005 deadline.

References

1. Heid DW, Chasteen J, Forrey AW. The Electronic Oral Health Record. J Contemp Dent Pract. 2002 Feb 15;3(1):43-54.
2. Chasteen J, Murphy G, Forrey AW, et. al. The Health Insurance Portability & Accountability Act and the Practice of Dentistry: Privacy and Confidentiality. J Contemp Dent Pract. 2003 Feb 15;4(1):59-70.
3. Chasteen J, Murphy G, Forrey AW, et. al. The Health Insurance Portability & Accountability Act and the Practice of Dentistry: Electronic Transactions. J Contemp Dent Pract. 2003 Nov 15;4(4):108-20.
4. http://cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp (Accessed May 17, 2004)
5. ADA Technical Report 1031 “Internet Security Issues for Dental Information Systems” 2003.

About the Authors

Joseph E. Chasteen, DDS, MA

Dr. Chasteen is an Associate Professor in the Department of Oral Medicine and serves as the Director of the Office of Educational & Information Technology at the University of Washington School of Dentistry in Seattle, Washington. He has authored several periodicals on the use of computers in dental practice as well as textbooks related to dental practice management.

Gretchen Murphy, MA

Gretchen F. Murphy Med, RHIA is Director and Senior Lecturer of the Health Information Administration Program, School of Public Health and Community Medicine at the University of Washington in Seattle, WA. She has represented the American Health Information Management Association in several health informatics standards activities and chaired the ASTM Technical Committee on Health Informatics' Subcommittee on the Structure and Content of the Electronic Health Record from 1992-2002. She has authored several books and book chapters on health information management subjects.

Arden Forrey, PhD

Dr. Forrey serves as a Research Associate in the Department of Restorative Dentistry, University of Washington School of Dentistry. He has served as the Veteran's Administration Decentralized Hospital Computer Project Site Manager at the Seattle VA Medical Center; a Research Fellow in Fleet Medical Informatics, US Navy Medical Research and Development Command, and in the Department of Pediatrics at Georgetown University.

David Heid, DDS

Dr. Heid is the former Chief of Dental Services at the Seattle Veterans Medical Center in Seattle, WA and now serves as a Clinical Professor in the Department of Restorative Dentistry at the University of Washington School of Dentistry. He has also held the position of an Associate Professor in the Department Restorative Dentistry at the Medical College of Georgia.

e-mail: dheid@cablespeed.com