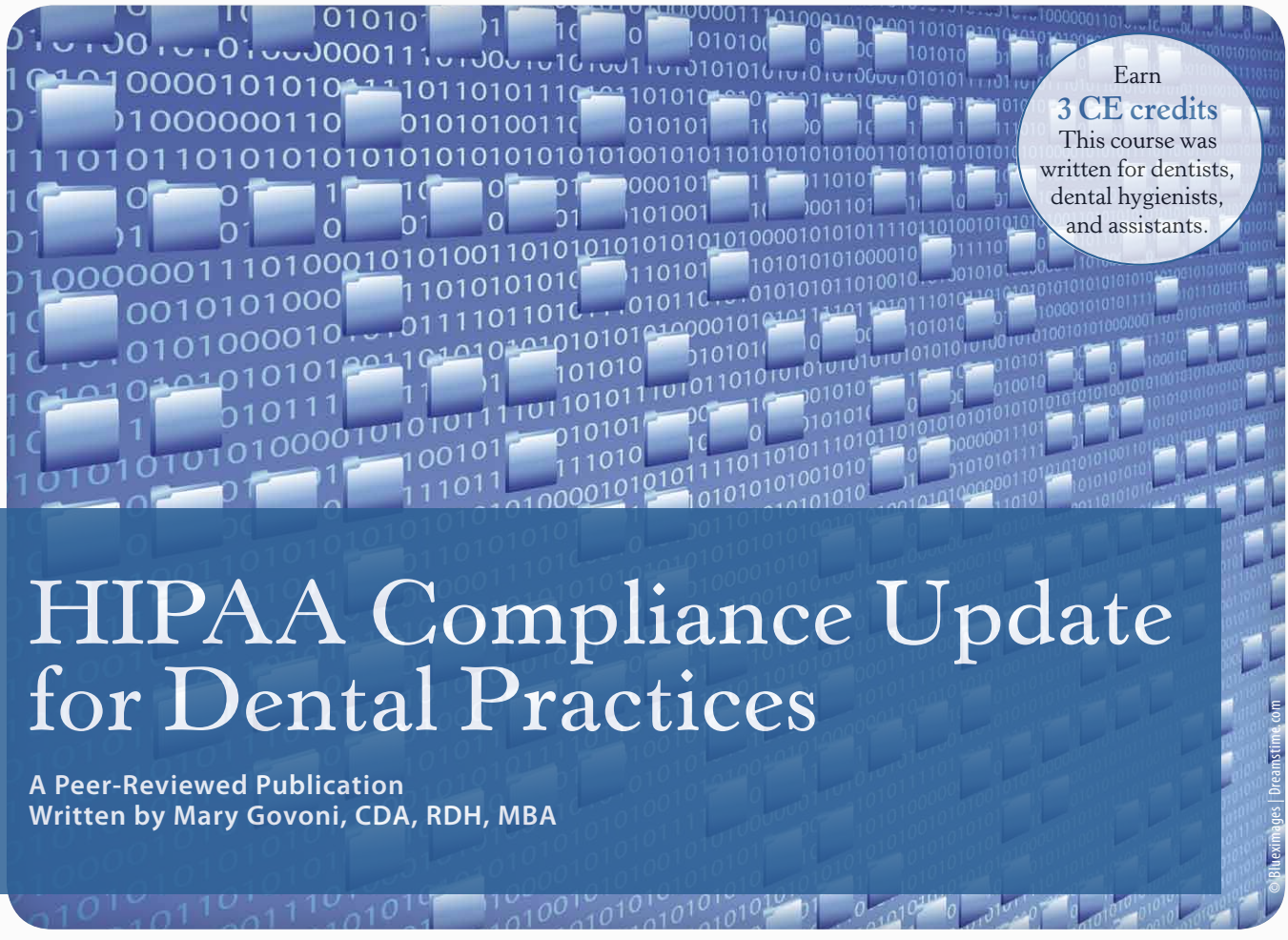

Earn
3 CE credits
This course was written for dentists, dental hygienists, and assistants.

HIPAA Compliance Update for Dental Practices

A Peer-Reviewed Publication
Written by Mary Govoni, CDA, RDH, MBA

Abstract

Compliance with HIPAA rules is essential for every dental practice from a risk management standpoint for the practice as well as for the security of the patients' protected health information. In order to comply with these rules dentists and dental team members must first understand the scope of the rules and how they apply to the delivery of oral health care services. This article describes the HIPAA Privacy and Security Rules and their application to both administrative and clinical protocols in a dental practice setting.

Educational Objectives

At the conclusion of this educational activity participants will be able to:

1. Identify the federal agencies responsible for promulgation and enforcement of HIPAA rules.
2. Identify protected health information and its uses and disclosures.
3. Describe the various types of HIPAA-required documentation needed in a dental facility.

Author Profile

Mary Govoni, CDA, RDH, MBA is an internationally recognized speaker, author and consultant on clinical efficiency, ergonomics, OSHA & HIPAA compliance, and team communication. Mary is a past president and life member of the American Dental Assistants Association, a member of the American Dental Hygienists Association, a consultant to the ADA Council on Dental Practice, a member of the Organization for Safety Asepsis and Prevention, the Academy of Dental Management Consultants and the Speaking and Consulting Network. She is a featured speaker on the ADA CELL seminar series and a columnist for Dental Economics magazine.

Author Disclosure

Mary Govoni, CDA, RDH, MBA has no commercial ties with the sponsors or the providers of the unrestricted educational grant for this course.

Go Green, Go Online to take your course

Publication date: Jan. 2015
Expiration date: Dec. 2017

Supplement to PennWell Publications

PennWell is an ADA CERP recognized provider

ADA CERP is a service of the American Dental Association to assist dental professionals in identifying quality providers of continuing dental education. ADA CERP does not approve or endorse individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry.

Concerns or complaints about a CE provider may be directed to the provider or to ADA CERP at www.ada.org/goto/cerp.

PennWell designates this activity for 3 continuing educational credits.

Dental Board of California: Provider 4527, course registration number CA# 03-4527-14098
"This course meets the Dental Board of California's requirements for 3 units of continuing education."

The PennWell Corporation is designated as an Approved PACE Program Provider by the Academy of General Dentistry. The formal continuing dental education programs of this program provider are accepted by the AGD for Fellowship, Mastership and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from (11/1/2011) to (10/31/2015) Provider ID# 320452.

This educational activity has been made possible through an unrestricted grant from Eaglesoft.

This course was written for dentists, dental hygienists and assistants, from novice to skilled.
Educational Methods: This course is a self-instructional journal and web activity.
Provider Disclosure: PennWell does not have a leadership position or a commercial interest in any products or services discussed or shared in this educational activity nor with the commercial supporter. No manufacturer or third party has had any input into the development of course content.
Requirements for Successful Completion: To obtain 3 CE credits for this educational activity you must pay the required fee, review the material, complete the course evaluation and obtain a score of at least 70%.
CE Planner Disclosure: Heather Hodges, CE Coordinator does not have a leadership or commercial interest with products or services discussed in this educational activity. Heather can be reached at hhodges@pennwell.com
Educational Disclaimer: Completing a single continuing education course does not provide enough information to result in the participant being an expert in the field related to the course topic. It is a combination of many educational courses and clinical experience that allows the participant to develop skills and expertise.
Image Authenticity Statement: The images in this educational activity have not been altered.
Scientific Integrity Statement: Information shared in this CE course is developed from clinical research and represents the most current information available from evidence based dentistry.
Known Benefits and Limitations of the Data: The information presented in this educational activity is derived from the data and information contained in reference section. The research data is extensive and provides direct benefit to the patient and improvements in oral health.
Registration: The cost of this CE course is $59.00 for 3 CE credits.
Cancellation/Refund Policy: Any participant who is not 100% satisfied with this course can request a full refund by contacting PennWell in writing.

Educational Objectives

Upon completion of this educational activity participants will be able to:

1. Identify the federal agencies responsible for promulgation and enforcement of HIPAA rules.
2. Identify protected health information and its uses and disclosures.
3. Describe the various types of HIPAA-required documentation needed in a dental facility.

Abstract

Compliance with HIPAA rules is essential for every dental practice from a risk management standpoint for the practice, as well as for the security of the patients' protected health information. In order to comply with these rules dentists and dental team members must first understand the scope of the rules and how they apply to the delivery of oral health care services. This article describes the HIPAA Privacy and Security Rules and their application to both administrative and clinical protocols in a dental practice setting.

Introduction

Many dental teams find that the HIPAA Privacy and Security Rules are confusing, ambiguous and get in the way of treating patients. This course will assist participants in understanding the history, purpose and scope of the HIPAA rules and assist in understanding how to meet the compliance requirements.

History of HIPAA

Passed by Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) had two goals. These goals were to help make the delivery of health care services for Americans more efficient and to increase the number of Americans who had health insurance coverage. In order to achieve these goals, it was determined that the use of electronic health information or records would provide the "administrative simplification" that was believed to be key to increasing health care coverage and making the delivery of health care services more efficient.[1] The Department of Health and Human Services (HHS), which was charged with implementing HIPAA, determined that regulations were needed to protect the privacy of health information. Thus, rules were proposed in 1999, and became effective in 2003, to regulate the types of uses and disclosures of personally identifiable health information by covered entities. Known as the HIPAA Privacy Rule, it took effect on April 14, 2003. Two years later, on April 15, 2005, the HIPAA Security Rule became effective. The Security Rule focuses on protecting the confidentiality, integrity and availability of electronic health information that is protected by the HIPAA Privacy Rule.

Covered entities, as defined by HIPAA, are health care providers who transmit any health information electronically including health plans (e.g. health insurance companies, Medicaid and Medicare programs) and health care clearing houses that process health care claims, among many others. Most dental practices fit the definition of covered entities.[2]

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) was passed as part of the American Recovery and Reinvestment Act (ARRA), and put forth incentives for the creation of a national health care infrastructure and the adoption of a system for electronic health records (EHR) among health care providers. The HITECH Act also broadened the scope of the privacy and security provisions already in force under HIPAA, as well as increasing the legal liability of covered entities for non-compliance with the rules and provided for greater enforcement of the rules. In 2013, the HIPAA Omnibus Rule was passed, which essentially combined the Privacy Rule, the Security Rule and the HITECH Act, plus some additional clarifications to the previous rules.[3]

Protected Health Information

Compliance with the HIPAA Rules centers around the definition and protection of health information, which is any information, whether oral or recorded in any form or medium that is created by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house. It also includes information that relates to past, present or future physical or mental health or condition of any individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual. A subset of health information is individually identifiable health information (IIHI) and it relates to the past, present and future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and that identifies the individual or where there is reasonable basis to believe that the information can be used to identify an individual.

Protected health information (PHI) is the information that dental practices use on a daily basis during the delivery of patient care. It is defined as individually identifiable health information (IIHI) that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. Patient information in a dental practice is protected health information (PHI) whether it is in electronic or paper format. The Privacy Rule covers PHI in any format; the Security Rule covers PHI in electronic format.[4]

Use of PHI

Protected health information (PHI) is utilized by dental practices in two distinct ways. The first, and most common is called treatment, payment and health care operations (TPO). It involves the numerous ways in which patient information is used and disclosed in the course of providing treatment. These uses include referrals to other dentists or health care providers, consultations between health care providers related

to treatment, billing, collections, eligibility determination and resolving benefit claims. When a patient signs their HIPAA acknowledgement form, they are granting the covered entity permission to use PHI for these purposes.

The other, less common use of PHI is non-TPO, which is related to marketing or using PHI for purposes other than treatment, such as the use of patient images on websites or in presentations. Patients must consent in writing to these types of uses of their PHI and a covered entity must disclose when and how the information is to be used. Patients can also request that a covered entity provide documentation of when and how PHI was used for non-TPO going back 6 years.

Oversight and Enforcement of HIPAA Compliance

Enforcement of HIPAA rules and compliance by covered entities is the responsibility of the Office for Civil Rights (OCR).[5] In 2012 a pilot program was implemented to randomly audit covered entities for compliance with the Privacy and Security rules, referred to as Phase 1. The Phase 2 audit program, scheduled for implementation between Oct. 2014 and June 2015, will include covered entities and business associates. If a health care provider or business associate is selected for an audit, they will be notified in writing by the OCR.

If a covered entity has a complaint filed by a patient, the OCR will investigate and potentially cite and fine the covered entity for violations of the Privacy or Security rules. Covered entities can also be sued in the civil courts for such violations. In addition, if a breach of electronic PHI (ePHI) occurs, the HHS protocol for Breach Notification may need to be implemented. This protocol will be discussed in detail later in this course.

Complying with HIPAA Rules

Compliance with the HIPAA rules includes training of the "workforce" or employees, written documentation of privacy and security policies and practices, acknowledgement from patients that they have been given access to the facility's privacy and security policies, posting of the Notice of Privacy Practices, implementation of both a disciplinary process for employees who may violate HIPAA rules, and a complaint process for patients who believe their PHI has been inappropriately disclosed, assessing and maintaining the security of electronic PHI, documenting any breaches of the security of PHI and notification of patients of security breaches if applicable.

Training

Employers are required to provide HIPAA compliance training to their employees when hired and to provide regular training refresher updates for existing employees. Records must be maintained to document the dates of training, the participants and the content covered in the training session. Training must be tailored to the specific job functions for each employee. Once training is completed, employees should sign a statement that they are aware of the practice's policies on the privacy and security of PHI and that they agree to follow the prescribed protocols for the practice. This statement should also include information for the employees on disciplinary actions that may be imposed for non-compliance with protocols.

Documentation

As a covered entity, a dental practice or facility must have a written "Notice of Privacy Practices", which summarizes the ways in which the practice may utilize PHI, the protocols that the facility uses to protect the PHI, and details the complaint process for patients to follow if they believe that the privacy or security of their PHI has been compromised. Patients and/or guardians of patients must be given access to the Notice of Privacy Practices (NPP), which is typically done by posting the document in an area accessible to all patients, such as the reception area. If patients request a copy of the NPP, it must be provided to them. The content of the NPP has changed since the initial implementation of the Privacy Rule in 2003. If a dental practice has not updated the NPP since the new Omnibus Rule became effective in September of 2013, it should be done as soon as possible. Sources for templates for the NPP are the Dept. of Health and Human Services (HHS) – www.hhs.gov, and the American Dental Association (ADA) – www.ada.org.

A covered entity must also have written Privacy and Security Policies[6], which describe in detail the policies and protocols that the practice or facility has in place to safeguard the privacy and security of PHI and electronic PHI. In these policies, a member of the workforce must be named as the privacy officer and the security officer, so that both employees and patients know whom they should contact if there are questions or complaints regarding compliance. Again, both the HHS and the ADA have templates available for documenting these policies in a dental practice.

Other items that must be documented in a dental practice include a "list of designated record sets",[7] which describes the types and locations of records and the location(s) where PHI is stored by a covered entity. For example, most dental practices have paper charts that are filed in the business office, and those charts are a designated record set, as well as the computer server where billing and financial information for patients is stored. The location of those records, both in the facility or possibly in an off-site facility must be documented, so that PHI can be accounted for at all times. Table 1 illustrates a typical list of designated record sets for a dental practice.

Table 1. List of Designated Record Sets

Record Sets	Location
Patient charts	File cabinet(s) in business office
Billing information	Computer server
Images	Computer server
Archived patient charts	Basement of building

Covered entities must have written Business Associate Agreements or BAA's with persons or companies who may have access to, use or disclose PHI as part of their responsibilities to the dental practice. These agreements are legal contracts that ensure that the business associate and their sub-contractors will follow appropriate protocols to protect the privacy and security of patient information that they may access. Examples of people or companies include attorneys, accountants, answering services, consultants (technology or business), collection agencies, software vendors and others. According to the ADA and the National Association for Dental Laboratories (NADL), dental laboratories are not included in this requirement, however many practices choose to have BAA's with their dental laboratories.

Dental practices must also have a written security risk assessment for their electronic PHI. This analysis must be a comprehensive review of the potential threats to the electronic or ePHI, and the safeguards that a facility has in place to prevent breaches of the data contained in the records. The safeguards fall into three categories: administrative, technical and physical. Administrative safeguards include written policies and protocols, technical safeguards include the use of internet security software and firewalls to protect from hackers, and physical safeguards include backing up data. HHS introduced a risk assessment tool (SRA) in 2014 that can assist dental teams in meeting this requirement. The tool can be accessed at http://www.HealthIT.gov/security-risk-assessment. An iOS version is also available from the Apple® App Store; search for HHS SRA tool. Any deficiencies identified in the security risk assessment must be addressed and corrected by the dental practice, since non-compliance can pose a risk for a security breach as well as a HIPAA citation and fine.

Other documentation required by HIPAA rules includes keeping logs of any privacy or security incidents, documenting the details of any privacy or security incidents, complaint forms for patients to complete if they feel that their PHI has been inappropriately used or disclosed, keeping logs of any patient requests for access to or requesting changes to their records and written records of assessments of any suspected breaches of ePHI.

Putting Compliance into Practice

Implementation of a HIPAA compliance program in a dental practice or facility requires time, resources and knowledge of the rules. A good place to begin is to compile a compliance manual; either paper or electronic. The items to include in the compliance manual are copies of the HIPAA rules, which are available from HHS at www.hhs.gov/ocr/privacy/hipaa/administrative/combined/, along with the Notice of Privacy Practices, Privacy Policy, Security Policy, Business Associate Agreements, and the Security Risk Assessment. As mentioned previously, the American Dental Association has templates for these items in their HIPAA Compliance Manual, available at www.ada.org.

Table 2 gives examples of additional steps for implementing a HIPAA compliance program.

Table 2.

Rule	Task
Privacy and Security	Appoint privacy and security officer; can be same person
Privacy and Security	Provide training and document training sessions
Privacy	Have patients sign updated (2013) acknowledgement form
Privacy	Post updated (2013) Notice of Privacy Practices
Security	Conduct security risk assessment, document in writing and update annually
Privacy and Security	Update Business Associate Agreements (2013)
Privacy and Security	Document list of designated record sets
Privacy and Security	Establish system to address violations and complaints
Security	Implement protocols/passwords to restrict access to ePHI
Security	Establish system for backup and restoration of ePHI
Security	Install and update internet security software and firewalls
Privacy and Security	Restrict the use of recording devices (cell phones/tablets) by patients and employees in clinical areas
Security	Encrypt server and practice management software
Security	Encrypt wireless network connections
Security	Use secure server for email communication
Security	Use encryption portal for transmission of patient information, such as radiographs
Security	Update computer operating software to a version that is supported by vendor (discontinue use of Windows XP®, since it is no longer supported by Microsoft®)
Privacy and Security	Update practice management software to a version that is HIPAA compliant
Security	Implement protocols for appropriate use of internet by employees in the workplace

Breach Notification

HIPAA defines a breach as any impermissible use or disclosure that compromises the privacy and security of PHI or ePHI[8]. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that although the PHI has been accessed in an unauthorized manner there is a low probability that the PHI has been compromised. This is determined by assessing what type of information was involved, what unauthorized person ac-

cessed the information, whether the information was acquired or viewed by an unauthorized person and the extent to which the risk was mitigated. If a covered entity discovers or suspects a breach of PHI, but determines that the unauthorized person who accessed the information would not be able to retain or access the information, the covered entity is exempt from breach notification.

For dental practices, this means that if all appropriate safeguards are in place to protect PHI and ePHI, such as passwords, and encryption of the server and email, the dental practice can be exempt from the breach notification process if an event occurs; since the practice put in place the required safeguards. If appropriate safeguards were not in place, the dental practice would be required to report the breach to HHS, notify all the affected patients, notify the media if more than 500 people were involved, and provide access to the credit reporting agencies for all affected patients if financial information was accessed, such as social security numbers.

Compliance with the Breach Notification Rule is a critical component of a HIPAA compliance program, since dealing with a breach can be costly to the practice as well as to the patients who might be affected.

Additional considerations for HIPAA compliance

Patient acknowledgement forms: This form is required by HIPAA for all patients and is their authorization for a dental health care provider to use their PHI in conjunction with their treatment[9]. When the patient or parent/guardian signs the form, they are giving their consent for the use of their PHI, and are acknowledging that they have had access to or been given a copy of the facility's Notice of Privacy Practices (NPP), which describes the ways in which their PHI might be used, and what security measures are in place to protect their information. Since the NPP was changed in 2013, patients should sign an updated acknowledgement form as of September 23, 2013. Keep in mind that patients who are 18 and older are legal adults, and must sign their own HIPAA form.

Electronic Health Records: Although much has been discussed regarding a mandate for electronic health records (EHR), as of the publication of this course, there is not a mandate for dental records to be electronic except in the state of Minnesota[10]. In medicine, providers will receive lower reimbursements under Medicare and Medicaid beginning in 2015 if their records are not electronic. It should be noted that although electronic records are not mandatory, they provide an important safeguard that paper records do not; the ability to easily back-up and restore the data. If paper records are destroyed or stolen they are most likely lost forever.

Verification of Identity: When patients present for treatment, dental practices should request to see a copy of a government issued identification card (except for children). Identity of telephone callers should also be verified, especially when a caller is inquiring about PHI. The caller can be asked to verify a birthdate, the last four digits of a social security number or other pertinent data.

Recall cards and sign-in sheets: HIPAA does not prohibit the use of recall cards and post card reminders, however, they cannot make any reference to a patient's PHI, such as necessary treatment. In other words, the recall or reminder card can say that a patient has or needs an appointment, but not what the appointment is for. Sign-in sheets can be used, provided that only the patient's name is listed and perhaps an appointment or arrival time. The sign-in sheet is not the appropriate place for the patient to list updates to their information, such as new phone number, address, benefit plan information, etc.

Treatment discussions: While HIPAA does not require treatment rooms to be enclosed or sound-proofed, health care providers are required to make reasonable accommodations for protecting patient privacy. Treatment should not be discussed in the reception area. It is best discussed in the operatory. It is a common practice for the dentist, hygienist or assistant to report recall visit findings to a parent in the reception room as a child is being dismissed. This is unacceptable if there are other people in the reception area who can hear the discussion.

Treatment and other information cannot be discussed with individuals other than the patient without their permission. In some situations a verbal consent is acceptable, in others, written consent is required. For example, if a spouse of a patient calls to inquire about payment that was made for treatment and wants details regarding the treatment, it cannot be disclosed without the patient's permission. If the patient is available to give verbal consent over the phone, it can be noted in the patient record. Written consent to discuss treatment with specific individuals can be obtained when the patient signs their HIPAA acknowledgement form.

Replacement of electronic devices: Electronic devices that store patient information, such as computer hard drives, back-up drives, digital printers and fax machines must have the hard drives removed and destroyed or reformatted to erase all existing data when they are replaced so that the data cannot be accessed. Using a drive scrubbing software program does not completely eliminate the data on the drive. Data remains on the drive until new data is saved in that particular sector on the drive. The drives should be removed and rendered unusable to prevent access to the data.

Use of the internet in a health care facility: A dental practice must have a written policy on the use of the internet on the computers for that facility. Using the computers for personal business, downloading files and accessing certain websites poses security risks to ePHI. Many social networking sites are frequently hacked and certain types of software, such as games, may have malware or spyware embedded, which may affect the practice's software and server. Unauthorized use of computers by employees should be prohibited and disciplinary procedures should be in place in the case of violation of this policy.

Sending and receiving email and email with patient information: Communicating with patients by email is not prohibited by HIPAA, but must be done through a secure server. Email is becoming more and more popular as an efficient method of confirming appointments and following up with patients after treatment, as well as providing an introduction to the practice for new patients. Email providers, such as Gmail®, Yahoo®, Hotmail® and AOL®, among others, are not secure email portals and are frequently hacked. Therefore using an unsecure email portal poses some security risks for health care providers. Many practice management software programs, website hosting companies and other software services can provide secure email portals for dental practices. Existing email addresses can be utilized through these portals.

If a dental practice is sending or receiving patient information, such as treatment referrals or x-rays, those emails must be sent as encrypted messages, since the source of the patient information comes from the patient database on the server. If the email were to be intercepted, a pathway or portal to the server could be accessed by a hacker and patient ePHI could be compromised. Likewise, opening unsecure messages with attachments can also provide an opportunity for unauthorized access to a patient database. Encryption of email can be facilitated through special services and through some practice management software programs.

Summary

Although HIPAA compliance seems to some to be a nuisance and additional unnecessary work, it is every patient's right to have their health care and other personal information protected and secure. Providing excellent care in a safe and secure environment is the responsibility of all dental health care workers. In light of all that is happening in today's world regarding the security of all electronic information, compliance with HIPAA requirements is not only a professional responsibility, but a necessary business practice.

Bibliography

1. 45 CFR Parts 160, 162, and 164.
2. 45 CFR 160.103.
3. Federal Register, Vol. 78, No. 17, January 25, 2013
4. 45 CFR Part 160, 45 CFR Part 164
5. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html
6. 45 CFR 164.530 (i)
7. 45 CFR 164.530 (j)
8. 45 CFR 164.530 (j)
9. 45 CFR 164.520
10. Minnesota Statute §62J.495 (Electronic Health Record Technology)

Author profile

Mary Govoni, CDA, RDH, MBA is an internationally recognized speaker, author and consultant on clinical efficiency, ergonomics, OSHA & HIPAA compliance, and team communication. Mary is a past president and life member of the American Dental Assistants Association, a member of the American Dental Hygienists Association, a consultant to the ADA Council on Dental Practice, a member of the Organization for Safety Asepsis and Prevention, the Academy of Dental Management Consultants and the Speaking and Consulting Network. She is a featured speaker on the ADA CELL seminar series and a columnist for Dental Economics magazine.

Author Disclosure

Mary Govoni, CDA, RDH, MBA has no commercial ties with the sponsors or the providers of the unrestricted educational grant for this course.

Notes

Notes

Notes

Notes

Online Completion

Use this page to review the questions and answers. Return to **www.ineedce.com** and sign in. If you have not previously purchased the program select it from the "Online Courses" listing and complete the online purchase. Once purchased the exam will be added to your Archives page where a Take Exam link will be provided. Click on the "Take Exam" link, complete all the program questions and submit your answers. An immediate grade report will be provided and upon receiving a passing grade your "Verification Form" will be provided immediately for viewing and/or printing. Verification Forms can be viewed and/or printed anytime in the future by returning to the site, sign in and return to your Archives Page.

Questions

1. Information contained in a patient's records is described in the HIPAA Privacy rules as:
   a. Confidential information
   b. Protected health information
   c. Accessible to patients
   d. Accessible to all health care providers
2. Patients must have access to which of the following documents regarding HIPAA rules?
   a. Privacy and security policies
   b. HIPAA acknowledgement form
   c. Informed consent for treatment
   d. Notice of Privacy Practices
3. The implementation of certain protocols when patient information has been accessed in an unauthorized manner is called:
   a. Security risk assessment
   b. Security breach
   c. Breach notification
   d. Notice of Privacy Practices
4. HIPAA rules are enforced by the:
   a. Dept. of Health and Human Services
   b. State dental board
   c. Office for Civil Rights
   d. Dept. of Justice
5. Employees must be provided with HIPAA training:
   a. Upon hiring and annually thereafter
   b. When they are hired by a dental practice
   c. When there has been a data breach
   d. On an annual basis or when there are changes
6. Business Associate Agreements apply to the following individuals that require access to patient information, except:
   a. Attorneys
   b. Accountants
   c. Consultants
   d. Cleaners
7. HIPAA requires health care providers to evaluate their protection of ePHI on an annual basis. This is known as a:
   a. Risk assessment
   b. Security policy
   c. Privacy policy
   d. Compliance assessment
8. Emails with patient information attached must be sent through:
   a. A secure website
   b. An encryption portal
   c. An email server
   d. A secure server
9. The HIPAA rules require that access to ePHI be restricted to only authorized users by using:
   a. Data encryption
   b. Audit trail review
   c. Unique passwords
   d. Security software
10. If a patient has a concern or complaint about the use or disclosure of their PHI, they should be directed to the:
    a. Office for Civil Rights
    b. Privacy Officer
    c. Security Officer
    d. Dept. of HHS
11. The use of Windows XP® operating software in dental practices is no longer HIPAA compliant because it:
    a. Can't be purchased after April 2014
    b. Isn't compatible with practice management software
    c. Isn't supported by Microsoft® after April 2014
    d. Isn't compatible with digital imaging equipment
12. The Notice of Privacy Practices (NPP) for dental practices must be updated as of Sept. 23, 2013 because:
    a. Changes to the rules that took effect on that date
    b. It must now be updated on an annual basis
    c. It expires every ten years
    d. The NPP doesn't need to be updated
13. The purpose of restricting the use of cell phones and other devices with cameras or recorders in clinical areas is to comply with HIPAA rules regarding the:
    a. Security of patient information
    b. Use of protected health information
    c. Privacy of patients during treatment
    d. Cell phone use does not need to be restricted
14. A protocol for backing up and restoring ePHI is required by which of the following rules?
    a. HIPAA Privacy
    b. HIPAA Security
    c. Breach Notification
    d. Medicaid certification
15. A dental practice must have written protocols that describe the appropriate use of the internet in a dental facility because inappropriate use can cause a:
    a. Violation of patient privacy
    b. Violation of office policy
    c. Security breach
    d. Network malfunction
16. A dental health care provider is allowed to donate or sell used computer equipment that may contain patient information if:
    a. The computer's hard drive has been scrubbed with a drive-erase program
    b. Patients have signed their HIPAA acknowledgement forms
    c. The server data has been encrypted
    d. The hard drive has been removed and destroyed
17. An important compliance requirement regarding workforce/employee HIPAA training is that it is:
    a. Presented during work hours
    b. Employees are paid for the training
    c. Approved for continuing education credit
    d. Documented with dates, names and topics discussed
18. If a dental practice is selected for a HIPAA audit, the result can be:
    a. Citations and fines
    b. Closing of the facility
    c. Breach notification
    d. Patients leave the practice
19. How would a dental practice be notified of a HIPAA audit?
    a. By a visit to the office by a compliance officer
    b. By written notification from the OCR
    c. The practice would receive a phone call from OCR
    d. The practice would receive a summons
20. It is important to verify the identification of new adult patients for HIPAA compliance primarily to prevent:
    a. Identify theft
    b. Security breaches
    c. Insurance fraud
    d. Privacy violations
21. It is acceptable to use patient sign-in sheets, provided that they:
    a. Are not visible to other patients waiting in the reception area
    b. Do not ask for information other than name and appointment time
    c. The information on the sheet is blacked-out with a marker
    d. Are shredded at the end of the day
22. A reminder post card can have the following information in addition to the patient name:
    a. Time of appointment
    b. Information about premedication
    c. Treatment to be rendered
    d. Time and treatment to be rendered
23. To protect patient privacy, treatment discussions should take place:
    a. Anywhere that the dental team has access to patient information
    b. In the reception area or in the treatment rooms
    c. Wherever the patient is comfortable having the discussion
    d. In the operatory, consultation room or a private office
24. To prevent data breaches, backups of patient information must be:
    a. Secured
    b. Encrypted
    c. Locked
    d. Updated
25. Operating software, such as Windows®, must be configured to download updates because most of the updates are:
    a. Required to keep the system up to date
    b. Required by the practice management software
    c. Security patches that prevent breaches
    d. Operating system updates are not required
26. If an employee intentionally discloses protected health information on a patient, what needs to take place?
    a. The patient should be encouraged to file a complaint
    b. The incident needs to be reported to the OCR
    c. It should be documented in the HIPAA manual and the employee's file
    d. It should be documented and the employee disciplined if necessary
27. When a patient turns 18, but is still on his/her parent's account in the dental practice, the patient needs to:
    a. Bring documentation that they are still eligible for dental benefits
    b. Do nothing as long as the parents agree that they are responsible
    c. Sign their own HIPAA form because they are now legally an adult
    d. Receive a copy of the Notice of Privacy Practices
28. The Notice of Privacy Practices must be:
    a. Made available to all patients upon request
    b. Mailed to all patients due to the updates to the NPP
    c. Signed by all patients
    d. Posted in the reception area
29. The types and locations of patient information that a health care facility has must be documented in a:
    a. Written privacy policy and protocols
    b. Written security policy and protocols
    c. List of designated record sets
    d. Inventory of electronic patient information
30. Business Associate Agreements (BAA's) must be updated:
    a. On an annual basis
    b. As of Sept. 23, 2013
    c. Every ten years
    d. No need to update

ANSWER SHEET

HIPAA Compliance Update for Dental Practices

Name: Title: Specialty:

Address: E-mail:

City: State: ZIP: Country:

Telephone: Home ( ) Office ( )

Lic. Renewal Date: AGD Member ID:

Requirements for successful completion of the course and to obtain dental continuing education credits: 1) Read the entire course. 2) Complete all information above. 3) Complete answer sheets in either pen or pencil. 4) Mark only one answer for each question. 5) A score of 70% on this test will earn you 3 CE credits. 6) Complete the Course Evaluation below. 7) Make check payable to PennWell Corp. **For Questions Call 216.398.7822**

Educational Objectives

1. Identify the federal agencies responsible for promulgation and enforcement of HIPAA rules.
2. Identify protected health information and its uses and disclosures
3. Describe the various types of HIPAA-required documentation needed in a dental facility

Course Evaluation

1. Were the individual course objectives met?

Objective #1: Yes No Objective #2: Yes No

Objective #3: Yes No Objective #4: Yes No

Please evaluate this course by responding to the following statements, using a scale of Excellent = 5 to Poor = 0.

2. To what extent were the course objectives accomplished overall?	5	4	3	2	1	0
3. Please rate your personal mastery of the course objectives.	5	4	3	2	1	0
4. How would you rate the objectives and educational methods?	5	4	3	2	1	0
5. How do you rate the author's grasp of the topic?	5	4	3	2	1	0
6. Please rate the instructor's effectiveness.	5	4	3	2	1	0
7. Was the overall administration of the course effective?	5	4	3	2	1	0
8. Please rate the usefulness and clinical applicability of this course.	5	4	3	2	1	0
9. Please rate the usefulness of the supplemental webliography.	5	4	3	2	1	0

10. Do you feel that the references were adequate? Yes No

11. Would you participate in a similar program on a different topic? Yes No

12. If any of the continuing education questions were unclear or ambiguous, please list them.

_____

13. Was there any subject matter you found confusing? Please describe.

_____

14. How long did it take you to complete this course?

_____

15. What additional continuing dental education topics would you like to see?

_____

If not taking online, mail completed answer sheet to

Academy of Dental Therapeutics and Stomatology,
A Division of PennWell Corp.
P.O. Box 116, Chesterland, OH 44026
or fax to: (440) 845-3447

For IMMEDIATE results,
go to www.ineedce.com to take tests online.
Answer sheets can be faxed with credit card payment to
(440) 845-3447, (216) 398-7922, or (216) 255-6619.

☐ Payment of $59.00 is enclosed.
(Checks and credit cards are accepted.)

If paying by credit card, please complete the following: ☐ MC ☐ Visa ☐ AmEx ☐ Discover

Acct. Number: _____

Exp. Date: _____

Charges on your statement will show up as PennWell

1.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	16.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
2.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	17.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
3.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	18.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
4.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	19.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
5.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	20.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
6.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	21.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
7.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	22.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
8.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	23.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
9.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	24.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
10.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	25.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
11.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	26.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
12.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	27.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
13.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	28.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
14.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	29.	Ⓐ	Ⓑ	Ⓒ	Ⓓ
15.	Ⓐ	Ⓑ	Ⓒ	Ⓓ	30.	Ⓐ	Ⓑ	Ⓒ	Ⓓ

AGD Code 148

PLEASE PHOTOCOPY ANSWER SHEET FOR ADDITIONAL PARTICIPANTS.

COURSE EVALUATION and PARTICIPANT FEEDBACK

We encourage participant feedback pertaining to all courses. Please be sure to complete the survey included with the course. Please e-mail all questions to: hhodges@pennwell.com.

INSTRUCTIONS

All questions should have only one answer. Grading of this examination is done manually. Participants will receive confirmation of passing by receipt of a verification form. Verification of Participation forms will be mailed within two weeks after taking an examination.

COURSE CREDITS/COST

All participants scoring at least 70% on the examination will receive a verification form verifying 3 CE credits. The formal continuing education program of this sponsor is accepted by the AGD for Fellowship/ Mastership credit. Please contact PennWell for current term of acceptance. Participants are urged to contact their state dental boards for continuing education requirements. PennWell is a California Provider. The California Provider number is 4527. The cost for courses ranges from $20.00 to $110.00.

PROVIDER INFORMATION

PennWell is an ADA CERP Recognized Provider. ADA CERP is a service of the American Dental association to assist dental professionals in identifying quality providers of continuing dental education. ADA CERP does not approve or endorse individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry.

Concerns or complaints about a CE Provider may be directed to the provider or to ADA CERP ar www.ada.org/cotocerp/

The PennWell Corporation is designated as an Approved PACE Program Provider by the Academy of General Dentistry. The formal continuing dental education programs of this program provider are accepted by the AGD for Fellowship, Mastership and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from (11/1/2011) to (10/31/2015) Provider ID# 320452

RECORD KEEPING

PennWell maintains records of your successful completion of any exam for a minimum of six years. Please contact our offices for a copy of your continuing education credits report. This report, which will list all credits earned to date, will be generated and mailed to you within five business days of receipt.

Completing a single continuing education course does not provide enough information to give the participant the feeling that s/he is an expert in the field related to the course topic. It is a combination of many educational courses and clinical experience that allows the participant to develop skills and expertise.

CANCELLATION/REFUND POLICY

Any participant who is not 100% satisfied with this course can request a full refund by contacting PennWell in writing.

IMAGE AUTHENTICITY

The images provided and included in this course have not been altered.

HIPCOMP0115PAT