Quality Resource Guide

HIPAA and the Dental Office

Author Acknowledgement

Rachel C. Kearney, BSDH MS

Division of Dental Hygiene
College of Dentistry
The Ohio State University
Columbus, Ohio

Rachel Kearney has no relevant relationships to disclose.

Educational Objectives

Following this unit of instruction, the learner should be able to:

1. Define HIPAA and its relationship to dental practices.
2. Define a covered entity.
3. Describe protected health information (PHI.
4. List the needed HIPAA policies and procedures for a dental office.
5. Define a breach and the actions needed after a breach occurs.
6. Explain their role in protecting health information.

MetLife designates this activity for **1.0 continuing education credits** for the review of this Quality Resource Guide and successful completion of the post test.

The following commentary highlights fundamental and commonly accepted practices on the subject matter. The information is intended as a general overview and is for educational purposes only. This information does not constitute legal advice, which can only be provided by an attorney.

Originally published May 2021. Expiration date: May 2024.

The content of this Guide is subject to change as new scientific information becomes available.

ADA C·E·R·P® | Continuing Education Recognition Program

MetLife is an ADA CERP Recognized Provider.
Accepted Program Provider FAGD/MAGD Credit **05/01/21 - 06/30/25.**

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.

Address comments or questions to:

DentalQuality@metlife.com

MetLife Dental Continuing Education
501 US Hwy 22, Area 3D-309B
Bridgewater, NJ 08807

Cancellation/Refund Policy:
Any participant who is not 100% satisfied with this course can request a full refund by contacting us.

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

This article is for informational purposes only and does not constitute legal advice.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect patient health information. The act was then implemented by the United States Department of Health and Human Services (HHS) by issuing HIPAA Privacy Rules. These rules address the use of individuals' health information, often called protected health information (PHI).[1] Since the law was passed in 1996, there have been many updates and additional rules that further define the set standards for health plans, healthcare clearinghouses, and healthcare providers who conduct electronic healthcare transactions. The overall goal of HIPAA is to allow the flow of health information to promote high-quality healthcare while assuring individual health information is protected.[2]

Compliance with the HIPAA rules is required for individuals, organizations or entities that meet the definition of a covered entity. A covered entity is any entity that transmits health information in electronic form in connection with the Secretary of HHS's adopted standards. The following are considered covered entities and are subject to the HIPAA Privacy Rules.

- **Healthcare providers:** Every healthcare provider who transmits information in an electronic form in which HHS has adopted a standard. These transactions include claims, benefit eligibility inquiries and referral authorization requests. Email communication in itself does not mean a healthcare provider is a covered entity.
- **Business associates:** If a covered entity has a business associate that accesses PHI, they also fall under the HIPAA rules. These associates may be contracted to do claims processing, data analysis, billing or other activities.

Examples of business associates:

- o A third-party administrator that assists with claims processing
- o A CPA firm whose account services involve access to PHI
- o An attorney whose legal services involve access to PHI
- o Consultants who access PHI

Contracts with business associates must include:

- Description of the permitted and required uses of PHI by the business associate
- Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law
- Require the business associate to use appropriate safeguards to prevent use or disclosure of PHI other than outlined in the contract
- Language indicating that if the covered entity knows of a breach or violation by the business associate that the covered entity is required to take steps to cure the breach or end the violation, and if this cannot be achieved the contract will be terminated
- If termination of the contract is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services Office for Civil Rights
- A sample contract for business associates can be found on the HHS site here: https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.
- Health plans: Entities that provide or pay for medical care such as health, dental, vision and prescriptions are considered covered entities. Health maintenance organizations (HMOs), Medicare and Medicaid fall in this category. Employer-sponsored health plans are also considered covered entities.
- Healthcare clearinghouses: Healthcare clearinghouses are entities that process healthcare information and put it into a standard form, usually for health plans or healthcare providers.[3]

The HIPAA law has evolved through the HIPAA Privacy Rules. HIPAA and the Privacy Rules have implications not only for medical offices and hospitals but also for all members of the dental team.

What information is protected?

The HIPAA rules protect all individually identifiable health information (held by a covered entity) in any form or media, including electronic, paper or oral information. This information can include demographic data such as name, address, birth date and social security number. Information related to an individual's past, present or future health condition and provision of health care for an individual is protected by HIPAA.[4]

The HIPAA rules do not limit all sharing of PHI. Some circumstances that PHI is permitted to be shared are:[4]

- To the patient directly
- To those whom the individual authorizes disclosure in writing
- For treatment of the patient
- Payments
- Health care operations (quality improvement activities, audits, etc.)
- In emergency situations
- As required by law or law enforcement purposes
- By public health authorities authorized by law
- Public interest and benefit activities including:[3]
  - o When required by law
  - o Public health activities
  - o Victims of abuse or neglect or domestic violence

- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement
- Functions concerning deceased persons
- Cadaveric organ, eye, or tissue donation
- Research, under certain conditions
- To prevent or lessen a serious threat to health or safety
- Essential government functions
- Workers compensation

Not only does HIPAA allow disclosure of PHI to the patient directly, but the HIPAA Privacy Rule requires a covered entity to act on an individual's request for access no later than 30 calendar days after the receipt of the request. If the covered entity cannot meet this deadline, they may have up to an additional 30 calendar days as long as it provides the individual, within the initial 30 day period, a written statement on the delay and a date by which the request will be completed.[5] Recently, the Office for Civil Rights has settled eighteen investigations on violations of this Rule. Consequences have varied but include fines from $30,000 to $200,000. [6]

HIPAA and Dentistry

Dental practices most commonly submit health data electronically, though if a practice does not, it is not required to follow the HIPAA rules. However, some dental provider contracts require compliance with HIPAA privacy regulations even if the practice is not considered a covered entity. It is a best practice, and strongly suggested by the American Dental Association that even if a dental provider is not considered a covered entity, they should implement all safeguards to protect PHI.[7]

It is important to remember that the HIPAA rules set the minimum standards required to protect PHI. States may have stronger laws than the HIPAA law, and a dental practice must ensure they meet both the HIPAA and the state laws.

Dental practices should establish clear privacy policies and procedures. Practices are required to appoint a privacy officer to ensure that the practice's policies are followed. An office manager or another member of the dental team may serve in this role. The privacy officer should have a thorough knowledge of the HIPAA Privacy and Security Rules. The privacy officer's duties may include; developing policies to ensure HIPAA compliance, documenting implementation of the policy, managing concerns related to privacy in the organization, developing or implementing HIPAA training, and monitor changes to the HIPAA rules and state regulations.[8] The HIPAA rules call for privacy training to be provided for all staff in the practice. The Department of HHS provides training materials on their website: https://www.hhs.gov/hipaa/for-professionals/training/index.html.[9]

HIPAA Privacy Compliance Checklist

- ✓ Create privacy policies and educate all staff on policies within the practice.
- ✓ Appoint a privacy officer.
- ✓ Prepare HIPAA Notice of Privacy Practices, distribute it to all patients and display it in the office.
- ✓ Have each patient sign to confirm they have been given the HIPAA Notice of Privacy Practices.
- ✓ Confirm appointments with the most limited amount of information.
- ✓ Sign-in sheets should list only name, time and provider (if necessary).
- ✓ Keep conversations at a volume that others cannot overhear.
- ✓ Have discussions about diagnoses and treatment in a reasonably private area.
- ✓ Keep information secure by locking computer screens when not in use and limiting information on printed schedules.
- ✓ Only share PHI when it is necessary for the treatment of the patient.
- ✓ A patient must provide written authorization for use or disclosure of PHI that is not for treatment, payment or other healthcare operations defined in the Privacy Rules.
- ✓ Ensure technology is up to date and provides options for encrypted data transmission.
- ✓ When disposing of any hard copy PHI, like film or paper, it should be shredded or destroyed so that the PHI cannot be read.
- ✓ Electronic media should follow the Guidelines for Media Sanitization when being disposed.

Patients also need to be informed of the privacy practices of the dental practice. A *Notice of Privacy Practices* which summarizes the office's privacy policies should be provided to the patients at or before their first appointment, and a signature should be obtained to confirm its receipt. In addition, practices should post this *Notice* in a public place within their practice.[10]

As most health records are now stored digitally, the HIPAA Security Rule establishes standards to protect an individual's electronic PHI (e-PHI). The first step in complying with the HIPAA Security Rule is to conduct a risk analysis. A risk analysis can reveal areas where the practice's PHI may be at risk. The following questions should be addressed during a risk analysis: has the office identified the e-PHI in the organization, what are the external sources of e-PHI, and what are the human, natural and environmental threats to information systems that contain PHI. HHS offers a tool on HIPAA Security Risk Assessment (https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool) to assist in compliance.[11]

HIPAA Violations and Consequences

A breach of PHI with policies and procedures in place may still occur. A breach is defined as *"an impermissible use of disclosure under the Privacy Rule that compromises the security or privacy of the protected health information."* If a covered entity identifies a breach, it must notify the affected individuals, the HHS Secretary and in some instances, the media. Covered entities must notify affected individuals within 60 days following the discovery of the breach. The following information should be included in the notification:

- Brief description of the breach
- Description of the types of information involved in the breach
- Steps the individual should take to protect themselves from potential harm
- Description of what the practice is doing to investigate the breach, mitigate harm, and prevent future breaches
- Contact information for the practice

The breach must also be reported to the HHS Secretary through the HHS Breach Portal. If the breach affects more than 500 people, the HHS Secretary should be notified no later than 60 days following a breach. If fewer than 500 people are affected, the practice can report the breach on an annual basis. If the breach affects greater than 500 residents of a state, the practice would also be required to provide notice to media outlets in the state. This notice could be a press release and would need to be provided within 60 days following the discovery of the breach.[12] Breaches of the HIPAA regulations can be costly. Civil and criminal penalties can include fines up to $25,000 for repeated violations of a standard within a calendar year and fines up to $250,000 and/or imprisonment for knowing misuse of PHI.[13]

As the implementation of the HIPAA laws and rules progresses, rules continue to evolve. It is essential that the privacy offer and the practice stay up to date on changes. Currently (2021), there are pending changes to the HIPAA Privacy Rule which would: allow a patient to inspect their PHI in person and allow them to takes notes or photograph PHI, change the maximum time to provide access to PHI from 30 days to 15 days, require posting of estimated fee schedules on websites, drop the requirement for obtaining written confirmation that a Notice of Privacy Practices was received, define an "electronic health record".[14] These changes have not been approved but demonstrate that the rules change and should be monitored.

Conclusion

The HIPAA laws and rules are essential in protecting patient privacy but can be complex for a dental practice to implement all the required standards. There are several resources provided by the American Dental Association that may be helpful in establishing dental office policies and procedures to comply with HIPAA laws and rules:

- ADA Complete HIPAA Compliance Kit. Available through the ADA Store. https://ebusiness.ada.org/productcatalog/product.aspx?ID=596.
- ADA Practical Guide to HIPAA Compliance: Privacy and Security Manual. Available through the ADA Store. https://ebusiness.ada.org/productcatalog/2020/HIPAA/J594BT,
- ADA Practical Guide to HIPAA Training. Available through the ADA Store. https://ebusiness.ada.org/productcatalog/595/HIPAA/The-ADA-Practical-Guide-to-HIPAA-Training/J596BT.

The HIPAA law and Privacy Rules were created to set a national standard for protecting health information. The dental team plays an integral role in compliance with the HIPAA Privacy Rules and protecting patients' health information. The HIPAA Privacy Rules are updated periodically; the appointed Privacy Officer should review these changes and make appropriate revisions to the practice's Privacy Policies. By following practices that reduce the risk of a breach of PHI, the dental office can protect the PHI of their patients and comply with the HIPAA Privacy Rules.

FAQ - Common Office Practices and HIPAA

Can our practice use sign-in sheets?

Dental practices are permitted to use sign-in sheets. The information collected on the sign-in sheet should be as limited as possible. A sign-in sheet could contain the patient's name, check-in time, and the provider's name if needed. It should not contain any medical information or reason for the visit.[15]

Can I still call out a patient's name in the waiting room?

Dental offices may still call out a patient's name in the waiting room. The HIPAA Privacy Rules allow for incidental disclosures that may occur as long as the practice uses reasonable safeguards and information.[15]

Can our practice leave a message for our patients?

Leaving a message for a patient can be done within the HIPAA rules. Only the minimum amount of information necessary should be left in a message. It is suggested by HHS to leave the provider's name and a number asking the patient to call back.[16]

Can our practice leave a message with a family member?

Yes, a practice can leave a message with a family member who answers the phone, and the patient is not home. Practices should use their best judgment and limit the amount of information that is shared. If the patient has asked for restrictions on this type of disclosure, a message should not be left.[16]

Can I discuss a patient's care with a family member?

You may talk with family members or friends of the patient about their care as long as the patient has had an opportunity to agree or object to sharing this information. Verbal permission from a patient is sufficient for speaking with a spouse, parent or child. A written form is not required though many practices choose to use a written authorization to document the permission.[17]

Can I hang a schedule up in the operatory?

A schedule can be hung in the operatory but should include limited information and be placed in an area where it is least accessible to those in the practice, *i.e.* inside the cabinet door.[18]

Can our office still send postcard reminders for recall visits?

Yes, dental practices can send communications to their patients via postal mail in the format of a postcard as long as the patient has not requested an alternative manner of communication. The Department of HHS considers a request to have mail sent in a closed envelope rather than by postcard a reasonable request that should be accommodated by a practice if requested.[16]

References

1. U.S. Department of Health & Human Services. HIPAA for Professionals. https://www.hhs.gov/hipaa/for-professionals/index.html (2017).
2. Cohen, I. G. & Mello, M. M. HIPAA and Protecting Health Information in the 21st Century. JAMA 320, 231–232 (2018).
3. Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA). (2018).
4. Office for Civil Rights. Summary of the HIPAA Privacy Rule. HHS.gov https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (2008).
5. Office for Civil Rights. 2050-How timely must a covered entity be in responding to individuals' requests for access to their PHI? HHS.gov https://www.hhs.gov/hipaa/for-professionals/faq/2050/how-timely-must-a-covered-entity-be/index.html (2016).
6. Office for Civil Rights. Resolution Agreements. HHS.gov https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html (2015).
7. Sfikas, P. M. HIPAA privacy regulations: new requirements for protecting patients' health information. Health Insurance Portability and Accountability Act. J. Am. Dent. Assoc. 1939 133, 1692–1695 (2002).
8. What are the Duties of a HIPAA Compliance Officer. HIPAA Journal https://www.hipaajournal.com/duties-of-a-hipaa-compliance-officer/.
9. Office for Civil Rights. HIPAA Training and Resources. HHS.gov https://www.hhs.gov/hipaa/for-professionals/training/index.html (2008).
10. Office for Civil Rights. For Small Providers, Small Health Plans, & other Small Businesses. HHS.gov https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/small-providers-small-health-plans-small-businesses/index.html (2008).
11. Office for Civil Rights. The Security Rule. HHS.gov https://www.hhs.gov/hipaa/for-professionals/security/index.html (2009).
12. Office for Civil Rights. Breach Notification Rule. HHS.gov https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (2009).
13. Chasteen, J. E., 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 Pr. 5, 158–167 (2004).
14. Adler, S. New HIPAA Regulations in 2021. HIPAA Journal https://www.hipaajournal.com/new-hipaa-regulations/ (2021).
15. Office for Civil Rights. 199-May providers use patient sign-in sheets or call out the names in their waiting rooms. HHS.gov https://www.hhs.gov/hipaa/for-professionals/faq/199/may-health-care-providers-use-sign-in-sheets/index.html (2015).
16. Office for Civil Rights. 198-May providers leave messages for patients at their homes to remind them of appointments. HHS.gov https://www.hhs.gov/hipaa/for-professionals/faq/198/may-health-care-providers-leave-messages/index.html (2015).
17. Office for Civil Rights. 2069-Under HIPAA, when can a family member of an individual access the individual's PHI from a health care provider or health plan? HHS.gov https://www.hhs.gov/hipaa/for-professionals/faq/2069/under-hipaa-when-can-a-family-member/index.html (2016).
18. HIPAA Rules for Dentists. HIPAA Journal https://www.hipaajournal.com/hipaa-rules-for-dentists/.

POST-TEST

Internet Users: This page is intended to assist you in fast and accurate testing when completing the "Online Exam." We suggest reviewing the questions and then circling your answers on this page prior to completing the online exam.

(1.0 CE Credit Contact Hour) Please circle the correct answer. 70% equals passing grade.

1. **HIPAA stands for:**
   a. Health Insurance Program Accountability Act
   b. Health Information Policy and Administration Act
   c. Health Insurance Portability and Accountability Act
   d. Healthcare Information Privacy and Action Act

2. **The purpose of the HIPAA Privacy Rule entity was to:**
   a. create national standards to protect patient information.
   b. create rules that medical and dental offices had to follow.
   c. make it more difficult to transmit health information.
   d. require health plans to cover more people.

3. **A _____ is a health provider, plan or clearinghouse that electronically transmits health information for which HHS has developed standards.**
   a. business associate
   b. privacy officer
   c. dental practice
   d. covered entity

4. **When is it permissible to share PHI under the HIPAA Rules?**
   a. In an emergency situation
   b. With advertising agencies
   c. With a friend of the patient
   d. On social media

5. **Which of the following are considered protected health information (PHI)?**
   a. Name
   b. Birthdate
   c. Diagnosis
   d. All of the above

6. **Are dental practices considered a covered entity?**
   a. Yes - all dental practices are considered covered entities.
   b. Yes - if they transmit electronic information in which HHS has created standards.
   c. No - only medical practices are considered covered entities.
   d. No - if there are less than two healthcare providers in the practice.

7. **A breach that affected 27 patients in your practice is required to be reported to the individual within**
   a. one calendar year.
   b. 60 days of discovering the breach.
   c. 24 hours of its occurrence.
   d. 30 days of reporting to HHS.

8. **Who in the dental office is required to be trained in the privacy policies?**
   a. Only the dentist
   b. Only the office manager
   c. Only the team members who submit insurance claims
   d. All members of the dental team

9. **When communicating with patients, a dental practice should implement which of the following?**
   a. Leaving detailed messages on a patient's voicemail.
   b. Calling out a patient's initials instead of their names in the waiting room.
   c. Using the least information possible if not speaking directly with the patient.
   d. Eliminating sign-in sheets.

10. **One way members of the dental team can protect health information is to:**
    a. closeout and/or lock computer stations.
    b. cover treatment information in the waiting room.
    c. share treatment information with all members of the team, even those not involved in the care.
    d. send letters instead of postcards to remind patients of their recall visits.

Registration/Certification Information (Necessary for proper certification)

Name (Last, First, Middle Initial): _____

PLEASE PRINT CLEARLY

Street Address: _____ Suite/Apt. Number _____

City: _____ State: _____ Zip: _____

Telephone: _____ Fax: _____

Date of Birth: _____ Email: _____

State(s) of Licensure: _____ License Number(s): _____

Preferred Dentist Program ID Number: _____ ☐ Check Box If Not A PDP Member

AGD Mastership: ☐ Yes ☐ No

AGD Fellowship: ☐ Yes ☐ No Date: _____

Please Check One: ☐ General Practitioner ☐ Specialist ☐ Dental Hygienist ☐ Other

FOR OFFICE USE ONLY

Evaluation - HIPAA and the Dental Office 1st Edition

Providing dentists with the opportunity for continuing dental education is an essential part of MetLife's commitment to helping dentists improve the oral health of their patients through education. You can help in this effort by providing feedback regarding the continuing education offering you have just completed.

Please respond to the statements below by checking the appropriate box, using the scale on the right.

	1 = POOR 1	2	3	4	5 = Excellent 5	
1. How well did this course meet its stated educational objectives?	☐	☐	☐	☐	☐	
2. How would you rate the quality of the content?	☐	☐	☐	☐	☐	
3. Please rate the effectiveness of the author.	☐	☐	☐	☐	☐	
4. Please rate the written materials and visual aids used.	☐	☐	☐	☐	☐	
5. The use of evidence-based dentistry on the topic when applicable.	☐	☐	☐	☐	☐	☐ N/A
6. How relevant was the course material to your practice?	☐	☐	☐	☐	☐	
7. The extent to which the course enhanced your current knowledge or skill?	☐	☐	☐	☐	☐	
8. The level to which your personal objectives were satisfied.	☐	☐	☐	☐	☐	
9. Please rate the administrative arrangements for this course.	☐	☐	☐	☐	☐	

10. How likely are you to recommend MetLife's CE program to a friend or colleague? *(please circle one number below:)*

10	9	8	7	6	5	4	3	2	1	0
extremely likely					neutral					not likely at all

What is the primary reason for your 0-10 recommendation rating above?

11. Please identify future topics that you would like to see:

Thank you for your time and feedback.

MetLife

To complete the program traditionally, please mail your post test and registration/evaluation form to:
MetLife Dental Quality Initiatives Program | 501 US Highway 22 | Bridgewater, NJ 08807