PRACTICAL GUIDE SERIES

Chapter 7

Training is the Key to Compliance

Chapter 7

Training is the Key to Compliance

HIPAA Training Overview

Since you have already provided HIPAA training to your staff, this chapter will serve as a strong basis for training refreshers on new HIPAA regulations such as Breach Notification, enhanced patient rights, and changes in your relationship with Business Associates.

If you are responsible for HIPAA training, this is your chapter. It is divided into the following components:

- HIPAA training requirements
- Sample topics for training refreshers
- A year-round calendar of HIPAA refresher training activities (Appendix 7-1)

What You're Required to Do

HIPAA Privacy, Security and Breach Notification Rules require training for all members of a dental practice's workforce, and training refreshers and updates as appropriate. Your HIPAA training responsibilities can build on the work you've already completed. For example, you should already have completed the following tasks:

- Conduct and periodically review your risk assessment
- Implement policies and procedures to safeguard patient information
- Conduct training for all workforce members based on those policies and procedures
- Update that training if policies and procedures change, and maintain compliance with evolving HIPAA regulations
- Document those activities

As you can see in Figure 7.1, updating and retraining your workforce is an ongoing process.

Figure 7.1 HIPAA Training is Ongoing

In previous chapters you learned how the HITECH Act strengthened HIPAA requirements to increase consumer confidence in health information technology. You also learned why it is important to develop and implement a HIPAA compliance program.

Your HIPAA training program should include all applicable topics necessary to bring your practice and workforce into compliance with HIPAA and applicable state law, and you must update your workforce training program as necessary, including any updates relevant to compliance with the 2013 Final Rule. The following sample training topics provide examples of ways to refresh your workforce training. However, the following sample topics are not intended to be, and should not be interpreted as, a substitute for a HIPAA training program or the training updates on the 2013 Final Rule.

Sample Training Update Topics

1. **Business Associates** (Chapter 1, Section 2.C and Chapter 2, Step 13)
   Your training program should cover the heightened policies and procedures you have implemented with Business Associates now that they must meet most HIPAA Privacy and Security requirements. Chapters 2 and 4 contain information regarding updated Business Associate requirements that dental practices can use as a tool in developing workforce training.

   a. Train staff on how your practice will work with Business Associates.

   b. Business Associates and their subcontractors must comply with most HIPAA Security Rule requirements.

   c. Train staff to immediately report to your Privacy Official any suspected activity or practice by a Business Associate that the staff member believes may violate HIPAA or the Business Associate Agreement so that the dental practice can take appropriate steps to fulfill its obligations under the HIPAA Privacy Rule.

   d. Train staff to immediately report to your Privacy Official any suspected or reported breach of patient information by a Business Associate (or anyone else), whether the breached information is in electronic, oral or hard copy form, so that the dental practice can take appropriate steps to fulfill its obligations under the Breach Notification Rule.

   e. Examples of Business Associates of a dental practice include billing services, software vendors, accountants, practice managers, and attorneys who access patient information while performing a service for the dental practice. Business Associate Agreements are also required for Health Information Organizations, e-prescribing gateways, and other providers of data transmission services that require access to patient information on a routine basis. A person or entity that stores patient information in paper or electronic form qualifies as a business associate. Vendors of personal health records acting on behalf of a dental practice are also business associates.

2. **Breach Notification Rule** (Chapter 1, Section 2.B and Chapter 2, Step 22)

   a. The federal government may impose penalties for failure to provide required notification for breaches of unsecured patient information that are discovered on or after February 22, 2010.

   b. Train workforce members to immediately report any suspected breach of unsecured patient information to the appropriate person in the dental practice. Workforce members who are responsible for encrypting patient information must understand how to use appropriate hardware and software to "secure" electronic patient information. Appropriate workforce members should be trained to investigate any suspected breach and to provide notification unless the dental practice can show that there is a low probability that the patient information was compromised based on an assessment of the relevant factors including, at a minimum, the following four factors:

      1. The nature and extent of the patient information involved, including the types of identifiers and the likelihood of re-identification

      2. The unauthorized person who used the patient information or to whom the disclosure was made

      3. Whether the patient information was actually acquired or viewed

      4. The extent to which the risk to the patient information has been mitigated.

c. The Breach Notification Rule discussion in Chapters 1 and 2 provides background that dental practices can use as a tool in developing workforce training. Breach Notification Rule training should include, but should not be limited to, the following topics:

- Electronic patient information must be encrypted according to applicable NIST standards in order to be deemed "secured." Workforce members should be trained not to disarm encryption as doing so may compromise the security or privacy of patient information.
- If "unsecured" patient information in any format (electronic, oral, or hard copy) is "breached" (as these terms are defined in the Rule), your practice is required to provide timely and appropriate notification to affected individuals, HHS, and, in some cases, the media. Examples of possible breaches include:
    1. An unencrypted electronic device is lost or stolen
    2. You inadvertently leave on a store counter a USB drive, portable computer or smart phone that is not properly encrypted
    3. A paper patient chart is poorly shredded and disposed of in the regular trash or recycling
    4. A hacker or disgruntled workforce member accesses patient information and uses it for financial gain
    5. A workforce member orally discloses information about a patient in violation of the HIPAA Privacy Rule
- If a breach of unsecured patient information involves 500 or more patients, your dental practice may be required to notify certain media outlets of the exposure, and you must provide notice to the Secretary of the U.S. Department of Health and Human Services without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.
- Properly encrypted electronic patient information is considered "secured." To help prevent breaches requiring notification, it is prudent to train workforce members about encryption, how it works, why they cannot shut it off, and penalties for doing so.
- The Breach Notification Rule requires Business Associates to notify the dental practice if the Business Associate discovers a breach of unsecured patient information. Train your workforce how to respond if a Business Associate notifies your practice that the Business Associate has discovered a breach. Train all workforce members to immediately notify the appropriate individual in your dental practice of any reported breach.
- In certain cases, conspicuous notice on the home page of your practice's website may be used to provide substitute notice if you lack contact information for 10 or more individuals involved in a breach. In the alternative, you may post a conspicuous notice in major print or broadcast media in the area where the 10 or more individuals likely reside. Train appropriate workforce members on your practice's methods of maintaining up-to-date patient contact information and the appropriate use of the practice's website and the media under the Breach Notification Rule.

3. **De-identifying patient information** (Chapter 2, Step 21)

    a. Train workforce members that:

        - *properly* de-identified patient information is not protected by HIPAA
        - disclosure of properly de-identified patient information will not result in a breach even if the information is not encrypted
        - an outside person or entity that performs a service for the dental practice involving only properly de-identified patient information is not a business associate of the dental practice and need not sign a business associate agreement

    b. Train appropriate workforce members to understand when it is appropriate to de-identify patient information. For example, the dental office hires a consultant who needs access to patient information but not to identifiers, de-identifying patient information before providing it to the consultant can decrease the dental practice's exposure to liability for a HIPAA violation (for example, by minimizing the likelihood of a breach).

    c. Train appropriate workforce members to properly de-identify patient information by removing the 18 HIPAA "identifiers" and confirming that the resulting information cannot be used, alone or in combination with other information, to identify the patient.

    d. Workforce members who are responsible for de-identifying patient information should not use "redaction" (for example, crossing out identifiers with a marker) to de-identify patient information. Redacted patient information is not "secured" under the Breach Notification Rule. It may still be possible to read redacted information. For example, when a document is scanned or photocopied, redacted information may become readable again. Identifiers should be removed using a more reliable method than redaction, and workforce members should confirm that the identifiers are not readable in hard copy, photocopy, or electronic format.

    e. Train workforce members in appropriate electronic and hard copy de-identification techniques.

4. **Patient Requests to Restrict Disclosures** (Chapter 1, Section 2.D and Chapter 2, Step 14.5)

    a. Train appropriate workforce members, especially those who are involved with billing, that patients have the right to restrict disclosure to a health plan if the dental practice is paid in full for the health care item or service.

    b. Other patient requests to restrict disclosures should be referred to the appropriate person in the dental practice (often the Privacy Official) who will determine whether to agree to the restriction. Train workforce members not to agree to such requests until directed by the Privacy Official, and to refer requests for restrictions to the Privacy Official for a decision.

5. **Marketing Communications and Sale of Protected Health Information** (Chapter 1, Sections 2.F and 2.G and Chapter 2, Steps 10 and 11)

    a. With certain exceptions, a dental practice must obtain prior authorization from patients before the dental practice makes a marketing communication if the dental practice receives "financial remuneration" (dollars) from a third party to make the marketing communication.

    b. With certain exceptions, a dental practice must obtain prior authorization from patients before the dental practice exchanges patient information for "remuneration" (payment or anything of value).

c. A dental practice does not need patient authorization before making a marketing communication in the form of in-person face-to-face communications and promotional gifts of nominal value, even if the dental practice is paid, as long as the communication is for a permissible purpose under HIPAA (treatment, case management, care coordination, or health plan benefits).

6. **Right to Electronic Access** (Chapter 1, Section 2.E and Chapter 2, Step 14.1)

   a. Under the 2013 Final Rule, if a dental practice maintains patient information in an electronic designated record set, a patient has the right to obtain a copy of his or her patient information in electronic format.

   b. If your practice maintains one or more electronic designated record sets, train appropriate workforce members to respond appropriately to a patient's request for an electronic copy of patient information.

7. **Stepped Up, Funded Enforcement Activities** (Chapter 1, Sections 1.D and 2.I)

   a. Prior to the HITECH Act, privacy and security enforcement activities were complaint-driven. Today, a HIPAA investigation or compliance review may be triggered if a patient complains to OCR about a dental practice's privacy practices, if a dental practice reports a breach of unsecured patient information, or if OCR otherwise learns of possible noncompliance by a dental practice (for example, if there is a news item about the dental practice). OCR also has the authority to conduct HIPAA audits that are not triggered by evidence of possible noncompliance.

   b. OCR may use civil money penalties collected from HIPAA violators to fund further enforcement activities.

   c. The HITECH Act permits state attorneys general to bring civil actions in federal court on behalf of state residents who have been harmed by a breach of patient information in violation of HIPAA.

8. **Increased Penalties**

   a. Make staff aware of the importance of correcting any HIPAA violation within 30 days. For some workforce members, that will mean retraining them to identify suspected violations and to report them immediately. For others, that will mean knowing how to investigate and correct violations. See Chapter 1 for a discussion of HIPAA and HITECH Act provisions relevant to this training topic that dental practices can use as a tool in developing workforce training.

   b. Explain to staff how the HITECH Act increased penalties for HIPAA violations and increased the liability of individuals who breach a patient's privacy. Explain your practice's internal sanctions that apply to workforce members who violate your HIPAA policies and procedures.

   c. Civil penalties for violating HIPAA have been restructured into tiers. The most severe penalties ($50,000 per violation) are for HIPAA violations due to "willful neglect" that are not corrected within 30 days. Somewhat lower penalties ($10,000 to $50,000) may apply if a violation due to willful neglect is corrected within 30 days. A violation due to reasonable cause (not willful neglect) can result in a $1,000 to $50,000 penalty. If a person did not know of a violation (and would not have known by exercising reasonable diligence), a penalty of $100 to $50,000 may result.

d. If a HIPAA violation continues for a number of days, (for example, if a dental practice lacks appropriate safeguards for a period of time) the number of identical violations may be counted on a per day basis. In many breach cases, OCR considers the number of affected individuals and HIPAA requirements violated.

e. There is an annual cap of $1.5 million for all violations of a specific HIPAA requirement or prohibition. However, noncompliance can result in violations of more than requirement or prohibition.

f. The law allows criminal penalties to be assessed against a dental practice workforce member who has abused his or her privileges to access patient information. Even merely looking at information about a patient out of curiosity can be a crime. An individual who knowingly obtains or discloses patient information in order to sell, transfer, or use the information for commercial advantage, personal gain or malicious harm can face fines up to $250,000 and/or imprisonment for up to ten years.

9. **Disaster Recovery and Contingency Planning** (Chapter 4, pages 29-36 and Chapter 5 pages 7-8)

   a. Train workforce on your disaster recovery and contingency plans.

   b. What should a workforce member do if he or she cannot access the electronic records?

   c. What are your disaster risks, what is the probability that they will occur, and what is your plan for managing those risks?

   d. Who should be notified, and when, in the event of a disaster?

10. **Security Reminders** (Chapter 4, pages 22-23)

    a. If it is reasonable and appropriate for your dental practice, create an ongoing security reminder program as part of your training program.

    b. Security reminders can be used to remind the workforce about required security activities such as:

       - Encryption
       - Protection from malicious software
       - Log-in monitoring
       - Password management

Appendix 7-1
Sample 12-Month Security Refresher Training Sessions

First month (45 minutes)	Second month (15 minutes)	Third month (12 minutes)	Fourth month (10-15 minutes)
Topic: **Breach Notification** Find a news clip about a security breach, and ask what would happen to the dental practice if this breach occurred in our dental office. Discuss Breach Notification Rule.	**Topic:** **Accounting of Disclosures and Restrictions** Discuss the six Patient Rights under HIPAA and the role of your Privacy Official. Train staff on the right of a patient to restrict disclosure to a health plan when the dental practice is paid in full for the item or service.	**Topic:** **Password Management** Provide a safe place for workforce to store passwords if they cannot remember them. For example, free or low cost software can be searched online using words such as password manager or password storage; more expensive solutions include a biometric authentication system that authenticates finger images and connects them to automatically stored passwords.	**Topic:** **Managing Patient Complaints** Your dental practice must have a process in place to receive complaints about the dental practice's privacy practices, and must designate (in writing) a person to receive complaints. All complaints must be documented. HIPAA prohibits intimidation or retaliation against anyone who makes a complaint. Discuss how complaints are handled at your dental practice.

Fifth month (10-15 minutes)	Sixth month (10 minutes)	Seventh month (20 minutes)	Eighth month (10 minutes)
Topic: **Permissible Uses and Disclosures** HIPAA permits a dental practice to use and disclose patient information in certain ways without having the patient sign an authorization form. Assign a permitted use or disclosure to each staff person and ask him or her to explain how it has been (or could be) used in your dental practice. Remind staff of your practice's HIPAA policies and procedures and where they are located.	**Topic:** **Managing Business Associates** Refresher for staff on Business Associate obligations to secure protected health information and to report breaches, and the obligation of both the dental practice and the business associate to have a written business associate agreement in place. Discuss possible Business Associate breaches and violations and what the dental practice would do to resolve the incident.	**Topic:** **Friends and Family Guidance** Present policies and procedures on how to verify a caller or person requesting information and friends and family guidance. Ask how the practice manages inquiries from friends and family.	**Topic:** **Internet Use** Present policies and procedures on checking email and online shopping using computers with patient information at the practice.

Ninth month (15 minutes)	Tenth month (60 minutes)	Eleventh month (20 minutes)	Twelfth month (60 minutes)
Topic: **Disclosures to Officials** Discuss procedures to follow when a public official requests information on a patient. Discuss confidentiality, patients' right to request restrictions on use and disclosure, and patients' right to request an accounting of disclosures.	**Topic:** **Disaster Recovery** Conduct a planned fire drill on a day when patients are not scheduled. Most fire departments will assist in this drill. Upon returning to the practice, imagine everything has been damaged or destroyed. What would you need to continue doing business? Make a list of small and large items, then modify your disaster recovery plan, if necessary, in light of what you learn from the drill. Build a Downtime Cabinet.[1]	**Topic:** **Marketing and Documentation** Discuss the rules on subsidized marketing communications and review your HIPAA compliance documentation. Re-evaluate your documentation process: • How are we doing on documentation? • Schedule an audit of documentation processes. • Assign teams to review policies and procedures to determine what needs to be updated.	**Topic:** **Year-end Evaluation** Report findings of internal audit (see Eleventh Month). Report findings on Notice of Privacy Practices, Business Associate, and policies and procedures teams. Report findings of forms and logs team. Evaluate training needs, particularly with new staff or staff with new responsibilities.

[1] A Downtime Cabinet contains essentials you are likely to need if your system goes down for more than 2-3 hours. These items may include paper pads, pens, a checkbook, a tamper-proof prescription pad, a list of local pharmacies, a billing encounter sheet with updated billing codes, dental referrals and system contacts information.

Appendix 7-1
Sample 12-Month Security Refresher Training Sessions

First month (45 minutes)	Second month (15 minutes)	Third month (12 minutes)	Fourth month (10-15 minutes)
Topic: **Breach Notification** Find a news clip about a security breach, and ask what would happen to the dental practice if this breach occurred in our dental office. Discuss Breach Notification Rule.	**Topic:** **Accounting of Disclosures and Restrictions** Discuss the six Patient Rights under HIPAA and the role of your Privacy Official. Train staff on the right of a patient to restrict disclosure to a health plan when the dental practice is paid in full for the item or service.	**Topic:** **Password Management** Provide a safe place for workforce to store passwords if they cannot remember them. For example, free or low cost software can be searched online using words such as password manager or password storage; more expensive solutions include a biometric authentication system that authenticates finger images and connects them to automatically stored passwords.	**Topic:** **Managing Patient Complaints** Your dental practice must have a process in place to receive complaints about the dental practice's privacy practices, and must designate (in writing) a person to receive complaints. All complaints must be documented. HIPAA prohibits intimidation or retaliation against anyone who makes a complaint. Discuss how complaints are handled at your dental practice.

Fifth month (10-15 minutes)	Sixth month (10 minutes)	Seventh month (20 minutes)	Eighth month (10 minutes)
Topic: **Permissible Uses and Disclosures** HIPAA permits a dental practice to use and disclose patient information in certain ways without having the patient sign an authorization form. Assign a permitted use or disclosure to each staff person and ask him or her to explain how it has been (or could be) used in your dental practice. Remind staff of your practice's HIPAA policies and procedures and where they are located.	**Topic:** **Managing Business Associates** Refresher for staff on Business Associate obligations to secure protected health information and to report breaches, and the obligation of both the dental practice and the business associate to have a written business associate agreement in place. Discuss possible Business Associate breaches and violations and what the dental practice would do to resolve the incident.	**Topic:** **Friends and Family Guidance** Present policies and procedures on how to verify a caller or person requesting information and friends and family guidance. Ask how the practice manages inquiries from friends and family.	**Topic:** **Internet Use** Present policies and procedures on checking email and online shopping using computers with patient information at the practice.

Ninth month (15 minutes)	Tenth month (60 minutes)	Eleventh month (20 minutes)	Twelfth month (60 minutes)
Topic: **Disclosures to Officials** Discuss procedures to follow when a public official requests information on a patient. Discuss confidentiality, patients' right to request restrictions on use and disclosure, and patients' right to request an accounting of disclosures.	**Topic:** **Disaster Recovery** Conduct a planned fire drill on a day when patients are not scheduled. Most fire departments will assist in this drill. Upon returning to the practice, imagine everything has been damaged or destroyed. What would you need to continue doing business? Make a list of small and large items, then modify your disaster recovery plan, if necessary, in light of what you learn from the drill. Build a Downtime Cabinet.[1]	**Topic:** **Marketing and Documentation** Discuss the rules on subsidized marketing communications and review your HIPAA compliance documentation. Re-evaluate your documentation process: • How are we doing on documentation? • Schedule an audit of documentation processes. • Assign teams to review policies and procedures to determine what needs to be updated.	**Topic:** **Year-end Evaluation** Report findings of internal audit (see Eleventh Month). Report findings on Notice of Privacy Practices, Business Associate, and policies and procedures teams. Report findings of forms and logs team. Evaluate training needs, particularly with new staff or staff with new responsibilities.

[1] A Downtime Cabinet contains essentials you are likely to need if your system goes down for more than 2-3 hours. These items may include paper pads, pens, a checkbook, a tamper-proof prescription pad, a list of local pharmacies, a billing encounter sheet with updated billing codes, dental referrals and system contacts information.