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.