



Tips for using the ADA Security Kit:

The task of security implementation can seem overwhelming at first, especially when reading the kit for the first time. Although the ADA strongly recommends that the practice owner read the whole Kit, or otherwise have a basic understanding of HIPAA Security, it is best to avoid reading the whole Kit from cover to cover at one time. Instead, read the Introduction, all of Chapter 1, and pages 19-35 of Chapter 2. These passages contain the keys to the rest of the text. To help with understanding some of the jargon, use the glossary on pages 163-167; remove these pages from the binder, clip or staple them together, and keep them handy while reading the text.

Keep in mind that HIPAA Privacy and HIPAA Security address two distinct parts of HIPAA, which impose separate regulatory requirements. Your approach to HIPAA Security, including how you staff compliance efforts, may vary greatly from how you handled HIPAA Privacy.

1. Your number 1 priority, after reviewing the key material described above, is to appoint your security official. Since a wide range of business decisions will need to be made in order to achieve security compliance, consider appointing a dentist owner or managing dentist as the security official.
2. After that, have your security official do the risk analysis in order to identify any weaknesses. This is the cornerstone of your HIPAA Security compliance efforts, and should be done thoroughly and supported as appropriate in your office by other staff and/or consultants.
3. During your risk analysis, prioritize the areas of weakness that put you at greatest risk and plan on addressing them before starting other tasks.
4. There are ADA Tips interspersed throughout the text; use them if they suit your practice.
5. The sample policies may or may not be appropriate for your practice; some dentists may find them to be overly complex. Use the sample policies as informational starting points and remember that you have the flexibility to write policies and implement safeguards that make sense for your practice's size, complexity, technical capabilities, and resources.
6. Don't be afraid to delegate certain tasks or seek input from your technology vendors when appropriate. Your software vendor or computer consultant may be particularly helpful to you as you work through Chapter 4, which deals with technical safeguards. You may wish to hear from more than one vendor to help assure you are heading in the right direction, and not doing more than you need to, unless you choose to do so for business or risk management purposes.



American Dental Association
www.ada.org

7. Use the MS Word Files on the CD-ROM to write and edit your policies. Consider using the track changes feature when writing the new policies. If you have not used the Track Changes before, consult your MS Word Help Files (F1 key on most computers; search for “Track Changes”).
8. Your security documentation may be stored electronically. Be sure you can retrieve it in any circumstances.
9. For your initial staff training, it is best to emphasize password protections, protections against malicious software, security reminders, and log in monitoring as the keystones of your security training. If it helps, use the MS PowerPoint presentation included in your Security Kit CD.
10. The twelve-session process in the training section of the Security Kit (Chapter 5) is not essential for staff education. You may choose to use this process for ongoing staff training in the future, after you have achieved security compliance.
11. As you use the ADA’s HIPAA Security Kit to assist you in complying with the security regulations, document what you do and why you believe it is appropriate.
12. Remember that making a good faith effort to comply, even if there will be room for improvement later, is a far better approach than doing nothing at all.
13. For general HIPAA information, contact the ADA at 800 621-8099, x4608, or email HIPAA@ada.org. Consult with your lawyer should you need specific legal advice.