Introduction

The American Dental Association's *Practical Guide to HIPAA Compliance* provides tools to help dental practices implement or update a HIPAA compliance program. HIPAA compliance helps protect your patients, your practice, and your assets.

"Getting Started" is a brief overview of HIPAA Compliance and touches on questions like:

- What is a HIPAA Covered Entity?
- What's the difference between the HIPAA Privacy Rule and the HIPAA Security Rule?
- How will HIPAA compliance help my practice?
- Is compliance difficult or expensive?
- What are the basic things I need to do?
- Is HIPAA flexible or do all dental practices comply with HIPAA in exactly the same way?
- What are the penalties for a HIPAA violation?

Chapter 1: The 2013 Final Rule discusses the new HIPAA rules that are effective on September 23, 2013, and how they are likely to affect dental practices. Some of the changes described in Chapter 1 include revising Business Associate Agreements and the Notice of Privacy Practices, changes to the Breach Notification Rule, patients' right to obtain electronic copies of electronic designated health records, patients' rights to restrict disclosure to a health plan when the dental practice is paid in full, and new enforcement penalties.

Chapter 2: 25 Steps Toward Privacy and Breach Notification Compliance goes through the HIPAA Privacy Rule step-by-step, with sample policies and procedures and sample forms to help you develop and implement a Privacy compliance program for your dental practice.

The HIPAA Privacy Rule gives patients certain rights over their health information, including dental records and billing records. For example, patients have the right to:

- See and get copies of their records
- Ask for a change in their records
- Get a list of certain instances when the dental practice disclosed their information
- Complain about the dental practice's privacy practices
- Ask the dental practice not to disclose their information
- Ask the dental practice to communicate with them confidentially, at an alternative location, or by an alternative means

Each of these rights has restrictions. Some of the most common restrictions are discussed in Chapter 2.

The Privacy Rule also covers matters such as:

- When and how a dental practice can use or disclose patient information
- When a written patient authorization is required for a use or disclosure and what it needs to say
- How to use, disclose, and request the "minimum necessary" amount of patient information
- Disclosures to your HIPAA business associates
- Situations involving minors, abuse and neglect, whistleblowers, and crime victims
- The Notice of Privacy Practices

Chapter 2 also includes information about the HIPAA Breach Notification Rule, which requires dental practices to provide notification of breaches of unsecured patient information to affected individuals, the federal government, and in some cases the media.

The Privacy Rule and the Breach Notification Rule apply to patient information in any form (including electronic, paper, films, and spoken information).

Chapter 3: Protected Health Information is a short chapter that defines "protected health information" ("PHI"). PHI is the kind of information protected by HIPAA. In general, PHI includes patient information in dental records and billing records. However, PHI can take other forms, and there are some exceptions to the definition of PHI, such as health information about employees that the dental practice holds in its role as an employer. Most of the time, PHI and "patient information" mean the same thing in a dental office. However, understanding how to identify PHI, and training your workforce to recognize and protect PHI, is critical to HIPAA compliance.

Chapters 4, 5, and 6 get into the nuts and bolts of the HIPAA Security Rule. The Security Rule is about protecting *electronic* patient information — for example, information in an electronic health record ("EHR"), on a laptop or desktop computer, on mobile devices, in an email, or on removable media like CD-ROMs and USB drives. Electronic information needs special protection because it presents unique vulnerabilities. For example, data can be hacked, laptops can be stolen, and USB drives can be misplaced. Encryption is an important example of a safeguard that can protect electronic patient information.

The HIPAA Security Rule requires a dental practice to conduct a written risk analysis and develop safeguards to protect electronic patient information. These safeguards are divided into three categories:

- administrative
- technical
- physical

The purpose of the Security Rule safeguards is to protect the *confidentiality, integrity,* and *availability* of electronic patient information:

- Confidentiality means that people can't access the information if they are not authorized to do so.
- Integrity means that the data is not corrupted, or changed without authorization.
- Availability means the data is there when you need it.

In addition to appropriate encryption, Security Rule safeguards include things like computer passwords, virus protection, data backup, facility security (like door locks), and workforce training.

Chapter 4: Administrative Safeguards is about security planning and workforce management and behavior.

Chapter 5: Technical Safeguards is about topics like encryption, automatic log-offs, and safely transmitting electronic data. You'll also learn important topics to keep in mind when talking to vendors about your IT needs.

Chapter 6: Physical Safeguards is about protecting patient information through rules on topics such as facility security, workstations, computer back-ups, reusable media, and disposal of electronic patient information.

Chapter 7: Training is the Key to Compliance discusses HIPAA workforce training and contains suggestions for conducting training on HIPAA topics. This chapter contains suggestions for twelve sample refresher training sessions. You'll also learn the importance of documenting your training efforts.

Chapter 8: 12 Key Things to Remember contains a summary with 12 key points to remember about HIPAA compliance, including training workforce members, breach notification, and federal government enforcement.

The sample policies, procedures, forms, and other documents are general in nature and serve as a starting point for you to customize your practice's compliance program. There is no "one size fits all" HIPAA compliance program. Your dental practice's policies and procedures will be the result of your own written risk assessment and the decisions you make about implementing reasonable and appropriate security measures for your practice.

Remember, you must document your policies and procedures, training records, and maintain certain logs and records, and retain each document for six years from the date of its creation or the date when it last was in effect, whichever is later. The federal government and certain state agencies can require you to produce this documentation — if you are selected for a HIPAA audit, you may be required produce it within as little as ten days. So be sure to keep the documentation organized, accessible, and up to date.

A word of caution: ***Do not simply copy or download the sample HIPAA Policies and Procedures or forms contained in the kit and adopt them as your own. You must first conduct your written risk assessment, and then you must develop policies, procedures, and forms that are appropriate for your practice.***

The information in this book is not a substitute for legal advice, and the sample policies, procedures, and forms are merely tools and examples. In the event of a civil or criminal inquiry, you will be held accountable for the policies and procedures you adopt for your practice, so you must to be sure your policies and procedures apply to the risks you will manage in your practice. The laws of your state may also come into play. For example, many states have data security laws with breach notification requirements that may overlap HIPAA.

As you go through this book, make a note of any "compliance gaps" that you come across — areas where your practice needs to improve in order to comply with HIPAA — and tackle the most important ones first. Be sure to enlist the help of qualified professionals, such as a qualified attorney licensed to practice in your jurisdiction. You may also decide to engage a technology consultant at some point, but after reading this book, you'll have specific reasons for that engagement.

Getting Started

Key Terms

Throughout this book, we use the following simplified terms:

HIPAA – When we refer to "HIPAA," we mean the HIPAA Privacy, Security and Breach Notification Rules.

Dental practice – When we refer to a "dental practice" we mean a dental practice that is a HIPAA covered entity. A dental practice is covered by HIPAA if it sends a "covered transaction," such as submitting a claim to a dental plan, in electronic form,[1] or if someone else (like a clearinghouse) sends an electronic covered transaction on behalf of the dental practice.[2]

Patient information – We use the term "patient information" in this book to mean "protected health information" ("PHI"). Most patient information is PHI, including dental records, health histories, billing records, radiographs, full-face photographs, and even "demographic" information such as patient's names, addresses, phone numbers, email addresses, genders, etc. For practical, everyday purposes, applying your HIPAA policies and procedures to any information about a patient is a good idea. But when you really need to figure out whether a specific piece of patient information is protected by HIPAA (for example, if you discover a suspected breach), the tools in Chapter 3 may help.

Patient – The HIPAA rules refer to "individuals." For a dental practice, this usually means the patient, and we use that term in this book. However, keep in mind that HIPAA protects information about both current and former patients, and that in some cases other people, such as a patient's legal representative, or the parents or guardians of minor children, have rights under HIPAA.

Appendix 1-1 contains a plain language glossary with simplified definitions. For more information, readers can turn to Appendix 1-2, which contains the official definitions.

[1] In electronic form means: using electronic media, electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

[2] For more examples of covered transactions and information about covered entities, see the Covered Entity Charts from the Center for Medicare & Medicaid Services. They are available at *http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf*.

This book is a tool that a dental practice can use as to develop a HIPAA compliance program, or to update an existing program. It contains basic information to get you started, whether you are developing your initial HIPAA compliance program or updating a program that goes back to 2003, when dental practices first needed to comply with HIPAA.

ADA® TIP

Dental practices that are HIPAA "covered entities" need to comply with the Privacy, Security and Breach Notification Rules. A dental practice becomes a covered entity when it sends certain transactions, such as claims, electronically. Most faxes are not considered electronic transactions.[3] A dental practice can become a covered entity if a dentist sends paper claims to a clearinghouse, and the clearinghouse converts those paper claims to an electronic format and submits them to a health plan on behalf of the dentist.

The Privacy Rule requires you to designate a "Privacy Official" to develop and implement your HIPAA privacy compliance program. The Security and Privacy Official can be the same person — for example, the dentist or the practice manager could fill both roles. Privacy policies and procedures must address a number of topics, including the "Notice of Privacy Practices," patient authorization forms, patient requests, logs, etc. Both the Privacy and Security Rules require workforce training. HIPAA Privacy requirements are discussed in Chapter 2, which also contains sample policies and procedures and sample forms.

A dental practice developing a new HIPAA compliance program may wish to develop Privacy and Security compliance simultaneously, because Security Rule compliance can take time. The Security Rule applies only to electronic patient information, both "at rest" (e.g., stored on a computer, on removable media, or off-site) and during transmission or receipt. Each element of the Security Rule is presented in Chapters 4-6, along with suggested policies and procedures. The Security Rule recognizes that safeguards for a solo or small group practice need not be as elaborate as the safeguards that a large provider, such as a hospital, should implement. Therefore, HIPAA Security gives you some *flexibility of approach* when developing your compliance strategy. The Security Rule requires you to designate a "Security Official," who is responsible for developing and implementing your HIPAA security compliance program.

Complying with HIPAA is an investment in the future of your practice. For example, a disaster recovery plan (or contingency plan), one of the Security Rule requirements, is good for your business. What would you do if a fire raged through your office? Do you know where your practice's insurance policies are kept? Have you ever conducted a fire drill? Could you set up temporary offices with a fellow practitioner? How would you access patient information?

ADA® TIP

HIPAA requirements for safeguarding protected health information have the added benefit of protecting your business assets.

Will HIPAA Compliance Be Difficult?

Some people are more comfortable with the HIPAA Privacy Rule because it is framed in familiar terminology and addresses familiar concepts, whereas the HIPAA Security Rule addresses technology and appears to contain technology jargon. But you won't have to be a "techie" to understand what's important about HIPAA Security. As you get to know the ins and outs of the Security Rule, you'll see that it's more about people, business planning, workforce management and behavior, and documenting your policies and procedures — many things that your practice is doing today — than it is about technical jargon.

After reading and working with this book, you'll become familiar with privacy and security requirements and you'll find that the task of developing and implementing your HIPAA compliance program is achievable. Dental offices and other small practices have flexibility to create reasonable and appropriate security procedures tailored to their size, complexity, capabilities, technical infrastructure and other factors.

Even a dental practice just getting started with HIPAA compliance may already be in compliance with some HIPAA Standards. For example, perhaps the practice already takes measures to safeguard patient information, and staff is trained to take certain steps to keep patient information confidential. Other dental practices may have HIPAA compliance programs that need updating to comply with the 2013 HIPAA final rule, and perhaps to encompass new technology and workflows. This book can help both kinds of practices understand their HIPAA compliance obligations.

The ADA Practical Guide to HIPAA Compliance: Privacy and Security Manual covers only federal, not state law. HIPAA generally supersedes state laws except those state laws that provide more "stringent" protection for patients or give patients greater access to their information. Check with qualified legal counsel to make sure you are in compliance with both HIPAA and any applicable state laws.

A Sensible Approach to HIPAA Security Compliance

Dental practices have many choices when deciding how to comply with the Security Rule. Those choices will begin after you've conducted your own individualized "risk assessment." A risk assessment is like a checklist that helps you identify your security exposures and determine how you will manage them. Once you've completed your risk assessment, you'll have a better idea of how to approach security compliance, and how to budget for implementation.

ADA® TIP

HIPAA's Security Rule is scalable. What's right for one dental practice may not be appropriate for another. Begin with a risk assessment. It's the only way for you to measure the tasks ahead.

Some dental practices develop and implement HIPAA compliance using in-house staff, and others choose to engage a security consultant. After you have evaluated your risks and reviewed this book, you should have a better idea about the kind of assistance you need.

Will HIPAA Security Compliance Be Costly?

If your computer systems and practice management software are relatively new, your budget may be more manageable than if you need up update legacy systems. However, if your risk assessment reveals that your patient information is vulnerable to unauthorized access, then the cost to comply will be an investment in the future of your practice.

Action Items

The following action items will help you through the process of becoming compliant and maintaining compliance.

1: Identify the Team.

Identify the persons in your practice who will be responsible for building your policies and procedures and for ongoing maintenance. These positions should be filled with workforce members with overall knowledge of the dental practice who will be available to manage compliance.

Privacy Official: Your Privacy Official is responsible for developing and implementing your HIPAA Privacy policies and procedures. He or she will need to understand patients' HIPAA rights and permissible uses and disclosures of patient information, be able to explain the Notice of Privacy Practices to patients who ask questions, and keep HIPAA forms and documentation organized.

Security Official: Your Security Official is responsible for developing and implementing safeguards to protect electronic patient information. Your Security Official must work closely with the Privacy Official; often they are the same person. Many security policies will overlap with privacy policies, and you want to make sure that your HIPAA privacy and security policies are consistent. Because implementation of the Security Rule will affect the business, personnel, and technological operations of your practice, in many practices the dentist may be the best choice to serve as Security Official.

HIPAA Team: In a small dental practice, the HIPAA team may include all or select employees of the practice. Your team may include your Practice Management Software representative, a technical consultant, and qualified legal counsel.

2: Develop and Implement your HIPAA Privacy Program.

Your Privacy Official is responsible for developing and implementing policies and procedures to comply with HIPAA Privacy and for updating your privacy program when necessary. Your initial compliance program will also include the development of any necessary forms, and implementing a system to retain documentation. Develop policies and procedures for complying with the HIPAA Breach Notification Rule as you develop your privacy program. Breach notification compliance will include procedures to identify, report, and assess suspected breaches, and to send notification when required.

3: Evaluate Your Practice for Security Risk (Risk Analysis).

The goal of the HIPAA Security Risk Analysis is to help you identify risks and vulnerabilities involving electronic patient information, and create appropriate security policies to manage those risks. The risk analysis is the heart of the Security Rule. You may find that your practice already has a number of security measures in place, but that you need a way to document those measures. You may also find vulnerabilities that need to be addressed through new safeguards. You are required to conduct an initial Risk Analysis and review and modify your security measures as necessary to continue to reasonably and appropriately protect your electronic patient information.

You can use the "Sample HIPAA Security Risk Assessment for a Small Dental Practice" in Appendix 4-2 as a basis for developing your Risk Analysis procedure. A large dental practice may find it appropriate to purchase a more detailed risk analysis program.

4: Make a Plan for Completing your HIPAA Security Compliance.

The Security Official should develop a plan and monitor the security team during the implementation and documentation of the project. Use the completed risk analysis to identify new office policies that are needed, and those that need to be updated. Establish realistic completion dates for your team. Remember that you may need to consult with your software or hardware vendors, so make sure that you allow enough time for those meetings.

5: Develop Written HIPAA Security Policies and Procedures.

Formally document the HIPAA Security Policies and Procedures that you determine are appropriate for your practice based on your risk analysis. Study the sample policies and procedures in Chapters 4-6 and use them as tools as you write HIPAA Security Policies and Procedures that apply specifically to your practice. You will need to tailor these sample policies for your practice.

6: Implement your HIPAA Security Policies and Procedures.

Some dental practices may choose to implement each policy and procedure as it is written, and some may choose to prepare and document in writing all policies prior to implementing any single policy. Keep in mind that some safeguards may be needed immediately to manage risks, and others may have a lower priority. Some policies will take longer to implement, or may require discussion with a vendor. You may find during the implementation process that a particular policy is written incorrectly and needs to be revised. You may also find that some policies are more difficult than anticipated and should be approached in a different way. Take the time to edit your written office policies when you make those discoveries. Make sure that you implement all policies that you have written.

7: Provide Workforce Training.

Now that you have written your HIPAA Privacy, Breach Notification and Security Policies, and you've implemented the procedures to fulfill those policies, every member of your workforce must be trained to follow the procedures. Chapter 7 has additional information about workforce training.

8: Develop Processes to Monitor your Policies.

Make sure to routinely review and update your policies as your practice operations change and as existing HIPAA regulations are modified. Ongoing maintenance is critical to continued compliance with HIPAA. Periodically review your dental office's risks, policies and procedures to determine whether your compliance program needs to be altered. Every dental practice changes over time. New computers or computer software may be purchased, employees may change functions in the office, or the office may grow in size. This can indicate a need to alter a policy or procedure, or update training.

ADA® TIP

Schedule periodic reviews of your HIPAA compliance program, evaluate technical and non-technical compliance, assess new risks and vulnerabilities, and consider any new HIPAA rules or new HIPAA guidance from the federal government. Update your compliance program accordingly, and update staff training.

Some Key Concepts of HIPAA Compliance

Flexibility of Approach

HIPAA allows a dental practice to use security measures that are reasonable and appropriate for the practice. Reasonable and appropriate are defined by the following criteria:

- Size, complexity, and capabilities
- Technical infrastructure, hardware, and software security capabilities
- The costs of security measures (Note: a zero budget is not an acceptable reason for failing to take reasonable and appropriate security measures)
- The probability and criticality of potential risks to electronic protected health information

ADA® TIP

Reasonable and Appropriate: The Framework for the Security Rule. There is no "one size fits all" HIPAA Security compliance program that is suitable for all dental offices.

Maintenance

The Security Rule requires that you periodically review the security measures that are in place to safeguard your electronic protected health information. Maintenance seems to get ho-hum reactions from most new Security Officials, but it is a significant, ongoing component of the rule. Security is never done.

You'll spend a good amount of time implementing the Security Rule in your dental practice, but it's the maintenance measures that will keep you in compliance.

ADA® TIP

Having up-to-date documentation and consistently enforced procedures will be important considerations if your practice is subject to a compliance audit or complaint investigation by the federal government.

Enforcement and Penalties

HIPAA civil money penalties and enforcement have become more severe. In addition, the federal government can impose criminal penalties on anyone who knowingly and wrongfully violates HIPAA by improperly using, obtaining, or disclosing patient information.

- **Civil Penalties**
  The 2009 HITECH Act significantly increased civil monetary penalties for failure to comply with the HIPAA Privacy, Security and Breach Notification Rules. Before HITECH Act, civil penalties were limited to $100 for each violation, up to a maximum of $25,000 for all violations of a given HIPAA requirement or prohibition in a single year. Today, violations can result in civil penalties ranging from $100 to $50,000 per violation, up to an annual maximum of $1,500,000 for all violations of a given HIPAA requirement or prohibition. Enforcement of these civil penalties applies to HIPAA violations occurring on or after February 18, 2009.

- **Criminal Penalties**
  An individual or entity that violates HIPAA can face the following criminal penalties for knowing, wrongful misuse of individually identifiable health information:

  - For knowing misuse of individually identifiable health information: A fine of up to $50,000 and/or up to one year in prison.
  - For misuse under false pretenses: A fine of up to $100,000 and/or up to five years in prison.
  - For offenses involving the sale, transfer or use of individually identifiable health information for profit or malicious harm: A fine of up to $250,000 and/or up to 10 years in prison.

Summary

It is very important for dental practices to develop and implement appropriate HIPAA compliance programs, to ensure that workforce members have been informed of the practice's HIPAA compliance policies and procedures and the consequences for violating them, and to impose applicable sanctions on workforce members who violate those policies and procedures. It is the law, and prudent business practice, to comply with HIPAA and safeguard your patients' information.