PRACTICAL GUIDE SERIES

Chapter 8

12 Key Things to Remember:

HIPAA Privacy, Security and Breach Notification

Chapter 8

12 Key Things to Remember: HIPAA Privacy, Security and Breach Notification

We have selected 12 key attributes of HIPAA Privacy and Security as reminders to help your practice and workforce members focus on HIPAA privacy and security on an ongoing basis, as part of your daily routine, as part of your business culture, and during staff meetings. We chose twelve attributes so that your dental practice can discuss one attribute a month during staff meetings, send a monthly email blast to workforce members, or post each in a monthly rotation on your practice bulletin board. Tailor the topics to what will be most effective in your dental practice.

Our discussion of these 12 key attributes is a general overview of certain compliance issues and is intended as a review and refresher. **However, it is not intended, and should not be interpreted as a substitute for the detailed information provided in the preceding chapters.** For a more complete understanding of the issues involved, refer to the applicable chapter of this volume and the appropriate statute or regulation, and consult qualified legal counsel.

The following twelve attributes are in no particular order.

1. Three Fundamental Properties of HIPAA Privacy and Security Rules

The three fundamental properties of HIPAA Privacy and Security are *confidentiality, integrity,* and *availability* of protected health information in any form:

Confidentiality means that patient information is not made available or disclosed to unauthorized persons or processes.

Integrity means that patient information has not been altered or destroyed in an unauthorized manner.

Availability means that patient information is accessible and useable upon demand by an authorized person.

2. Definition of Protected Health Information

HIPAA applies to *protected health information.* The definition of *protected health information* starts with the definition of *individually identifiable health information*[1].

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

1. is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

[1] 45 CFR 160.103.

(i) that identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information is individually identifiable health information that is:

(i) transmitted[2] by electronic media;

(ii) maintained[3] in electronic media; or

(iii) transmitted or maintained in any other form or medium,

and is not certain education records[4] or employment records held by a Covered Entity in its role as employer.

Protected health information includes genetic information. It does not include information about patients who have been deceased for more than 50 years. Patient information that is properly de-identified is not considered protected health information and is not protected by HIPAA.

3. Protected Health Information Identifiers

Make sure that your workforce members are aware of the following list of eighteen identifiers. If all eighteen identifiers (with respect to the patient and relatives, employers, or household members of the patient) are removed, the information is not considered protected health information, unless the dental practice has actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. The eighteen identifiers are:

- Names (including initials)
- Any geographic subdivision smaller than a state (including address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code[5])
- All elements of dates directly related to an individual (including a birth date, treatment date, etc.) except year, all ages over 89, and all dates, including year, that indicate ages over 89
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical or dental record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers

[2] Data in motion.
[3] Data at rest.
[4] Education records covered by the Family Educational Rights and Privacy Act ("FERPA"), as amended, 20 U.S.C. 1232g and records described at 20 U.S.C. 1232g(a)(4)(B)(iv).
[5] The geographic unit formed by combining all zip codes with the same three digits must contain more than 20,000 people; otherwise, the three-digit code must be changed to "000."

- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers such as finger and voice prints
- Full face photographic and any comparable images
- Any other unique identifying number, characteristic, or code, except that our dental practice may assign a code or other means of record identification to allow the information to be re-identified by our dental practice, as long as:
    - The code or other means of record identification is not derived from, or related to, information about the individual and is not otherwise capable of being translated so as to identify the individual, and
    - Our dental practice does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the code or mechanism for re-identification.

4. HIPAA Security Rule Attributes

The HIPAA Security Rule pertains to electronic protected health information. Here are some facts about the HIPAA Security Rule that you must know:

- The Security Rule is a set of standards and implementation specifications with which your dental practice must comply. Your Business Associates and their subcontractors who have access to patient information must comply with most of the Security Rule.
- The Security Rule *standards* always require compliance by your dental practice, while implementation specifications can be *required or addressable*.[6]
- The Security Rule is *scalable,* taking into consideration the size of your dental practice, and *flexible,* taking into consideration the structure of your practice, the costs of security measures, and the likelihood and criticality of potential risks to electronic protected health information that your practice may encounter.
- The Security Rule is intended to be *reasonable* and permits your dental practice to implement security measures that are *appropriate*.
- The Security Rule is based on the key principles of *confidentiality, integrity,* and *availability* pertaining to your dental patient's electronic protected health information.
- The Security Rule is *technology neutral:* your practice's choice of safeguards (inputs) is up to the practice as long as safeguard performance measures (outputs) are achieved.[7]

[6] Addressable does not mean "optional." Rather, an addressable implementation specification means that a dental practice must assess whether the implementation specification is a reasonable and appropriate safeguard for that dental practice, when analyzed with reference to its likely contribution to protecting the entity's electronic protected health information. Then the dental practice must either implement the implementation specification if it is reasonable and appropriate or, if it is not reasonable and appropriate, the practice must document why not, implement an equivalent alternative measure if reasonable and appropriate, and document the equivalent alternative measure.

[7] However, remember that, unlike the Security Rule, the Breach Notification Rule is ***not*** technology neutral. A dental practice must provide the required notifications if "unsecured" protected health information is breached. HHS specifies the technologies and methodologies for "securing" protected health information. See Chapter 1 Section 2.2.B and Chapter 2 Step 22 for information about the Breach Notification Rule.

- The Security Rule is based on *risk analysis* and *mitigation of risk:* you must identify potential *vulnerabilities* and *threats* to your electronic protected health information and implement risk avoidance measures.
- The Security Rule is built on a foundation of safeguarding electronic protected health information, so electricity is necessary to maintain the availability of electronic patient information. If electric power is down, a dental practice may require a back-up generator to make electronic patient information available.
- It is likely that your practice has already implemented and uses on a daily basis many of the policies and procedures that are formalized in the Security Rule and its standards, implementation specifications, and documentation requirements.
- The Security Rule represents prudent business operation behavior and is an investment in the future of your dental practice as a successful business.

5. Nine Critical Steps in the Security Risk Analysis

When your dental practice conducts its initial or updated risk analysis, refer to the following nine steps, which are outlined in Chapter 4 (pp. 4-5) and amplified in Appendix 4-2:

- Inventory electronic patient information at your dental practice.
- Gather information about how your practice uses electronic media for patient information, and how your practice stores and transmits electronic patient information.
- Identify realistic threats.
- Identify potential vulnerabilities.
- Assess current security controls.
- Determine likelihood and impact of a threat exploiting a vulnerability.
- Determine level of risk.
- Recommend security controls.
- Document risk assessment results.

6. Privacy and Security Awareness Training

Here is an overview of the HIPAA training requirements:

- **Privacy**. Your dental practice must train its workforce members on the policies and procedures required by the HIPAA Privacy Rule and the Breach Notification Rule.
    - Current workforce members must be retrained within a reasonable period of time whenever their "functions are affected by a material change in the policies or procedures required by the HIPAA Privacy Rule and the Breach Notification Rule."
    - New workforce members must be trained "within a reasonable period of time" after the person joins your dental practice. However, training new workforce members before permitting them to access patient information may help protect the dental practice from the consequences of breaches and HIPAA violations.
    - Your dental practice must document that training has been provided.

- **Security Awareness.** Implement a security awareness and training program for all members of [your dental practice] workforce (including management). The following addressable implementation specifications are addressable: [8]
    - Periodic security updates
    - Procedures for guarding against, detecting, and reporting malicious software
    - Procedures for monitoring log-in attempts and reporting discrepancies
    - Procedures for creating, changing, and safeguarding passwords

Here are suggestions as to how to conduct your required training:

- Allocate time at each staff meeting to address privacy and security.
- Examples of topics to consider at staff meetings might include your dental practice's policies related to:
    - Logging in to multiple workstations
    - Auditing user access to workstations
    - Detecting security incidents and breaches
    - Prohibition on posting or sharing of passwords
    - Encrypting electronic protected health information
    - Protecting against unauthorized access to patient information in various formats
- Institute formal training for current workforce members as to new or changed policies when policies are added or changed and applicable training whenever a workforce member changes jobs within the practice or takes on new job responsibilities. A dental practice may be prudent to provide annual training refreshers to all workforce members.
- Institute formal training for new workforce members within a reasonable time after they join the dental practice. It may be prudent to provide training before a new hire has access to patient information.
- Consider whether training courses on privacy and security, with tests to document understanding of privacy and security rules, would enhance your practice's risk mitigation efforts and compliance with HIPAA training requirements.[9]
- Consider posting reminder signs near workstations, in the break room, and other areas in your practice facility where workforce members gather.

[8] When an implementation specification is addressable, the dental practice must assess whether the implementation specification is reasonable and appropriate and determine whether it would likely contribute to protecting the practice's electronic protected health information. If so, then the dental practice must implement the specification. If the implementation specification is not reasonable and appropriate, the dental practice must implement an equivalent alternative measure if it is reasonable and appropriate. The dental practice must document the decision and the reasoning for whatever the practice implements.

[9] The *ADA Practical Guide to HIPAA Training* includes two levels of training: Level 1 teaches the basics of HIPAA compliance to dental office staff. Level 2 is a more detailed module intended for managers who are developing and implementing their office's HIPAA compliance Privacy and Security.

7. Enhanced HIPAA Enforcement

The HITECH Act and 2013 Final Rule significantly enhanced HIPAA enforcement and increased penalties for noncompliance. See Chapter 1 for information about HIPAA enforcement civil money penalties. Under the HITECH Act, penalties are substantially increased and have been divided into four tiers, with a maximum penalty of $1.5 million for all violations of an identical provision in a calendar year. The tiered penalties now range as follows, for each violation:

- $100 – $50,000 if the Covered Entity ***did not know*** and, by exercising reasonable diligence, would not have known, that it violated such provision.
- $1,000 – $50,000 if the violation was due to ***reasonable cause*** and not to willful neglect.
- $10,000 – $50,000 if the violation was due to ***willful neglect*** and was ***corrected*** as required.
- $50,000 if the violation was due to ***willful neglect*** and was ***not corrected*** as required.

Information about HIPAA violations and enforcement actions can be found in *HIPAA Enforcement* on the website of the Office for Civil Rights, *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html*.

8. Securing Electronic Protected Health Information

In 2009, HHS published the Breach Notification Interim Final Rule. Contained within this document is the very important *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals,*[10] which instructs your dental practice — and your hardware and software vendors — how to secure your practice's protected health information in storage (in your database or offsite), in transmission, or in disposal. Breach notification is not required for patient information that is properly secured. Securing patient information can help prevent the potentially devastating financial and reputational damage that can result if a dental practice's patient information is breached.

[10] 74 *Federal Register* 42742-42743.

Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

a. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

   i. Valid encryption processes for data at rest [your practice's database] are consistent with NIST Special publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*[11] [12]

   ii. Valid encryption processes for data in motion [your practice's electronic transmissions] are those which comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations;* 800-77, *Guide to IPsec VPNs;* or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.[13]

b. The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

   i. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or other otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

   ii. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitation,*[14] such that the PHI cannot be retrieved."

ADA® TIP

We recommend that you encrypt your electronic protected health information in storage and in transmissions so that it is "secure" as defined in the *Guidance*. We also recommend that you follow the protected health information disposal requirements outlined in the *Guidance*. Be alert to any changes in the provisions of the *Guidance,* because HHS can revise the *Guidance* from time to time. Such changes are likely to be announced on the *Health Information Privacy* webpages of the Office for Civil Rights: *http://www.hhs.gov/ocr/privacy*.

[11] NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available.
[12] Available at *http://www.csrc.nist.gov*.
[13] Available at *http://www.csrc.nist.gov*.
[14] Available at *http://www.csrc.nist.gov*.

9. Business Associates Must Comply with the HIPAA Security Rule

Your dental practice's Business Associates must comply with most provisions in the HIPAA Security Rule. As a covered entity, your practice is not required to enforce a Business Associate's compliance with the Security Rule. Rather, your dental practice may permit a Business Associate to create, receive, maintain, or transmit electronic protected health information on your behalf only if your dental practice enters into a compliant Business Associate agreement with the Business Associate.

10. Is Certification a Substitute for Compliance?

HIPAA requires ***compliance*** by the dental practices, Business Associates, and subcontractors to which it applies. It does not require that their workforce members obtain ***certification*** of their compliance from an external source. Compliance is an ongoing effort, whereas certification generally is considered a snapshot in a moment of time.

As of this writing, the federal government has not established or endorsed a certification process for HIPAA compliance. Covered entities, Business Associates and subcontractors are free to enlist the services of outside entities to assess their compliance with HIPAA, and certification may be a useful compliance tool, depending on how rigorous the program is. However, certification does not guarantee compliance. "Certified" persons and entities are still subject to enforcement by the federal government.

HIPAA training certification is not required, and a dental practice's HIPAA training obligations would not be satisfied by a single training episode, whether or not it resulted in certification.

11. Build Your Dental Practice Disaster Recovery Plan

The Security Rule "Contingency Plan" safeguard requires each dental practice and Business Associate to build a disaster recovery plan. This safeguard is required, not addressable.

As part of the "disaster recovery plan" requirement, dental practices and their Business Associates must "establish (and implement as needed) procedures to restore any loss of data [e.g., electronic protected health information]." The content and procedures of your dental practice's disaster recovery plan will depend on your practice's risk analysis: specifically, your disaster recovery plan will focus on the potential threats and vulnerabilities that your practice might experience in a disaster, as identified in your risk analysis. Has your Security Official assigned a practice team to respond if there is a disaster and do members of the team know what to do should a disaster trigger required action? Has your practice simulated a disaster to test readiness should a disaster occur?

Your dental practice, and in particular, your Security Official, should prepare a comprehensive, usable, and effective disaster recovery plan, which will take time and which will involve the entire workforce. Your dental practice's loss of electricity for a sustained period of time should be considered a disaster, affecting both your dentistry tools and your electronic patient information. How would your practice deal with such a disaster, and how long would it take for your practice to recover? Is another source of electricity available? Does your practice use secure off-site data backup?

"The ... [Security] rule calls for covered entities to consider how natural disasters could damage systems that contain electronic protected health information and develop policies and procedures for responding to such situations. We [HHS] consider this to be a reasonable precautionary step to take since in many cases the risk would be deemed to be low."[15] Even though the probability of occurrence may be low, your dental practice should consider potential losses that could result from any vulnerability or threat in a worst-case scenario.

12. Breach Notification Rule Enforcement

On February 22, 2010, the federal government began enforcing the HITECH Act Breach Notification Rule for breaches discovered on or after that date. If your dental practice has secured electronic patient information according to the *Guidance* that we discussed earlier in this chapter (#8, *Securing Electronic Protected Health Information*), then your practice will not be required to provide notification if the appropriately secured patient information is lost or stolen. Notification is only required if "unsecured" protected health information is breached.

Generally, a *breach* means the acquisition, access, use, or disclosure of unsecured protected health information in a manner that is not permitted under the HIPAA Privacy Rule. When a dental practice discovers a breach of unsecured protected health information, the dental practice must notify affected individuals, the U.S. Department of Health and Human Services, and, in some cases, the media, unless the dental practice can demonstrate that there is a low probability that the information has been compromised based on a written analysis of the relevant factors, including at least the four required 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

Information that does not include any of the eighteen the HIPAA "identifiers"[16] is not considered "protected health information" (unless the dental practice has actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information). Unauthorized use or disclosure of information that is not protected health information does not constitute a "breach."

There are three exceptions to the definition of "breach." One involves the *acquisition, access or use* of patient information, and the other two involve *disclosures* of patient information. Examples of these exceptions are in *The Three Exceptions to the HIPAA Definition of a Breach* (Chapter 2, Step 22).

The Breach Notification Rule is triggered when protected health information is disclosed to, or is accessed, acquired or used by, an unauthorized person. A dental practice that suspects a breach of unsecured protected health information should promptly investigate and determine whether notification is required, and must send any required notification without unreasonable delay and in no case later than 60 calendar days after discovering the breach.

[15] 68 Federal Register 8351.
[16] 45 CFR 164.514(b)(2)(i). For more information about protected health information and the HIPAA Identifiers, see Chapter 3.

Consider the potential adverse financial impact of a breach of unsecured patient information, including the cost of investigating and assessing the incident, technical and forensic analysis, legal and professional advice, and the cost of preparing and sending any required notification, as well as the cost in staff time. Consider also the reputational damage a breach of patient information could cause to your dental practice. Balance these costs against the cost of "securing" your electronic patient information by encrypting it using the technologies and methodologies specified in the *Guidance* discussed in this chapter. Securing your electronic patient information enhances its privacy and security and decreases the likelihood that your dental practice will be required to send notifications under the Breach Notification Rule.

We highly recommend that your dental practice consider encrypting your electronic patient information according to the *Guidance,* and make sure that all portable or mobile devices have installed encryption so that your practice will not be required to provide breach notification if such devices are missing, lost, or stolen.