PRACTICAL GUIDE SERIES

Chapter 1

The 2013 Final Rule

What You Will Learn in This Chapter

- Identify certain changes to HIPAA in the 2013 Final Rule
- Understand certain changes that the 2013 Final Rule will require dental practices to make to existing HIPAA compliance programs
- Action steps to help dental practices come into compliance with the 2013 Final Rule

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 patients' 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 (such as 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.

The following terms are key to understanding the content of this chapter.

Breach
Business associate
Disclosure
Genetic information
Marketing
Subcontractor
Unsecured
Use
Willful neglect

[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.*

Chapter 1

The 2013 Final Rule

Introduction

On January 25, 2013, the federal government published changes to the HIPAA rules that will require covered dental practices to update their compliance programs.

Effective and Compliance Dates

The changes are effective March 26, 2013, but dental practices have until September 23, 2013 to come into compliance. A dental practice may choose to become compliant with the new requirements before September 23, 2013, but the government will not penalize dental practices for noncompliance with the new requirements prior to September 23, 2013.

All business associate agreements entered into on or after January 25, 2013 must be compliant with the new requirements by September 23, 2013, but a transition period until September 22, 2014 applies to certain agreements that were in place on January 25, 2013 (see Section 2.C below).

The increased civil money penalties discussed in Section 2.J below have been in effect since 2009, and apply to HIPAA violations occurring on or after February 18, 2009.

This chapter will discuss the changes in the 2013 Final Rule that are most likely to impact dental practices, beginning with a brief history of HIPAA.

Contents:

A. Purpose of the law

Congress passed the HIPAA law in 1996 to require national standards for electronic health care transactions and code sets. Since Congress recognized that advances in electronic technology could erode the privacy of health information, Congress added provisions to the law requiring Federal privacy protections for patient health information. These provisions led the government to adopt the HIPAA Security and Privacy Rules. These rules have been strengthened over time. For example, the 2009 HITECH ACT required the Breach Notification Rule and other enhancements to HIPAA that were intended to enhance public confidence in the privacy of patient information as health care providers increased their use of electronic health record (EHRs). Many of the HITECH enhancements are embodied in new regulations issued on January 25, 2013 ("the 2013 Final Rule"). This chapter discusses the changes in the 2013 Final Rule that are most likely to affect dental practices.

B. Compliance dates

Dental practices were required to comply with the Privacy Rule beginning in 2003. Security Rule compliance began in 2005. In 2009, the Breach Notification Rule came along, and the government increased penalties for HIPAA violations and strengthened HIPAA enforcement. The compliance date for the changes in the 2013 Final Rule is September 23, 2013 (with a longer period to revise certain business associate agreements).

C. State law

A dental practice's HIPAA program must comply with both HIPAA and applicable state law. If a state law *is not contrary* to HIPAA, a dental practice must comply with both HIPAA and the state law. If a state law *is contrary* to HIPAA, a dental practice must comply with the state law if the state law is "more stringent" than HIPAA. In general, a state law is more stringent than HIPAA if the state law relates to the privacy of patient information and provides greater privacy protection for patient information or greater rights to patients with respect to that information.

For example, HIPAA requires a dental practice to act within 30 days if a patient asks to see or get copies of certain patient information (see Section 2.E below and Chapter 2, Step 14.1). If a state law requires a dental practice to act on such a request in a shorter time frame, it would be more stringent than HIPAA.

A dental practice should consult a qualified attorney in the appropriate jurisdiction to make sure the dental practice's HIPAA compliance program is compliant with both HIPAA and other applicable laws.

D. Enforcement

Federal government enforcement of HIPAA used to be complaint-driven. For example, if a patient complained to the federal government that a dental practice was not complying with HIPAA, the government could investigate and may impose penalties or a corrective action plan. While this is still the case, the federal government now has expanded enforcement responsibilities and has the authority to conduct HIPAA audits that are not generated by a patient complaint or other information indicating possible noncompliance. The federal government may also investigate breaches that are reported to the U.S. Department of Health and Human Services ("HHS") in accordance with the Breach Notification Rule. The Office for Civil Rights, an agency of HHS, is responsible for federal HIPAA enforcement.

In addition to federal enforcement, the HITECH Act of 2009 gave state attorneys general the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. State attorneys general have the authority to obtain damages on behalf of state residents and to enjoin further violations of the HIPAA Privacy and Security Rules.

For more information about HIPAA enforcement, including information about the enforcement process and examples of enforcement activities, visit the Office for Civil Rights, *HIPAA Enforcement* at *http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html*. Information about the audit program is available at Office for Civil Rights, *HIPAA Privacy & Security Audit Program, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html*.

E. Penalties

In the beginning, civil money penalties for a dental practice that did not comply with HIPAA were limited to $100 or less per violation, up to an annual cap of $25,000 for all violations of the same HIPAA requirement or prohibition. Today, there are tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirement or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a minimum penalty of $50,000 per violation.

2. Summary of Changes in the 2013 Final Rule

A. Notice of Privacy Practices

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 3

Background: HIPAA requires dental practices to provide patients with Notices of Privacy Practices ("NPPs") that explain how the dental practice may use and disclose patient information and some of the rights that patients have to control their information.

New rule: The new rule changes the content that must be included in the NPP. The new requirements are included in the sample NPP in Appendix 2.3.1 Here is an outline of some of the new provisions that must be in the NPP:

Authorization forms. Under the new rule, the NPP must contain information about patient authorization forms (Chapter 2, Step 9). The revised NPP must:

- describe the types of uses and disclosures that require a patient to sign an authorization form,
- contain a statement that other uses and disclosures not described in the NPP will be made only with the patient's written authorization, and
- contain a statement that the patient may revoke an authorization at any time, as long as the patient does so in writing, but:
    - o if the dental practice has already relied on the authorization to use or disclose patient information the revocation cannot apply to those uses or disclosures, and
    - o if the authorization was for purposes of obtaining insurance coverage, other law gives the insurance company certain rights.

Fundraising. If the dental practice plans to use patient information in order to raise funds for the practice (see "Fundraising"), the NPP must include a statement telling patients that the dental practice may contact them for fundraising, and that patients have the right to opt out of fundraising communications. The NPP may describe the mechanism for opting out, but this is optional. If the dental practice does not plan such fundraising activities, the NPP does not need to have this provision (however, the NPP would need to be revised if the dental practice plans to begin fundraising).

Restricted disclosure to a health plan. A dental practice needs to change the statement in the NPP about a patient's right to ask for a restriction on uses and disclosures of their information. Under the prior rule, the statement said that the dental practice had the final say when a patient asked the dental practice not to use or disclose the patient's information in a certain way. Under the new rule, the NPP must state that the dental practice does not have to agree if a patient asks the dental practice not to use or disclose the patient's information in a certain way, *except* if the following two criteria are met:

- if the patient asks the dental practice not to disclose information about a health care item or service to a health plan for payment or health care operations purposes, and
- the dental practice has been paid in full for the item or service by the patient or by another on behalf of the patient.

For example, if a patient pays cash for new dentures and asks the dental practice not to submit a claim to the patient's dental plan, the dental practice must comply with the patient's request.

Breach notification. The dental practice must state in the NPP that the practice is required by law to notify affected individuals following a breach of unsecured patient information.

Marketing and sale of PHI. A dental practice's NPP must be changed to advise patients that the practice cannot sell patient information without the patient's express written authorization, and that authorization is also required for certain marketing communications.

Psychotherapy notes. Most dental practices will not record or maintain psychotherapy notes. However, if the practice does so, the NPP must include a statement about special authorization requirement for uses and disclosure of psychotherapy notes.

ACTION STEPS:

- ☐ Review existing NPP.
- ☐ Revise to comply with the new rule, and with any changes in privacy practices.
- ☐ Have NPP forms accessible to LEP and disabled patients, as applicable.
- ☐ Effective date of revised NPP must be no later than September 23, 2013.
- ☐ By the effective date of the revised NPP:
  - ☐ post the revised NPP in a clear and prominent location in the dental office,
  - ☐ have copies of the revised NPP available for any patients who ask for a copy, and
  - ☐ if the dental practice has a website, replace the prior NPP with the revised NPP.
- ☐ Re-train staff to distribute revised NPP to first-time patients at their first appointment, and ask patients to sign an acknowledgement of receipt.
- ☐ Continue retaining a paper or electronic copy of the prior NPP for at least six years from the date when it last was in effect.

B. Breach Notification

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 22.

Compliance Date: September 23, 2013.

Background. When a dental practice has a breach of unsecured patient information, the Breach Notification Rule requires the dental practice to notify affected patients, HHS, and in some cases the media. The notices must contain certain required information. The rule also requires dental practices to have policies and procedures for discovering, assessing, and responding to potential breaches, and maintain a "breach log" to document and track breaches (see Appendix 2.22.2).

Generally, a "breach" is a use or disclosure of patient information that violates the Privacy Rule. There are three exceptions to the definition of a "breach," which are in the sample breach assessment form in Appendix 2.22.1.

If a business associate of a dental practice discovers a breach, the business associate must notify the dental practice. The dental practice must determine whether notification is required and must send any required notification letters (unless the business associate agreement delegates this responsibility to the business associate or to different business associate such as a law firm or breach response firm). However, ultimately the dental practice is responsible for ensuring that the business associate fulfills this responsibility.

Prior rule: The prior rule did not require notification unless the impermissible use or disclosure posed a *significant risk of financial, reputational or other harm to the individual.* This was referred to as the "harm standard."

New rule: The new rule replaces the harm standard with a "compromise standard," which focuses on the probability that the patient information was compromised. A dental practice must send breach notification *unless* it 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, and
4. The extent to which the risk to the patient information has been mitigated

The sample breach assessment form in Appendix 2.22.1 incorporates the four factors.

A dental practice now has the discretion to provide the required breach notifications following an impermissible use or disclosure of patient information without performing a risk assessment. Under the 2013 Final Rule, there is a presumption that a breach has occurred following every impermissible use or disclosure of patient information, so dental practices may decide to notify without evaluating the probability of the compromise.

Examples: A dental practice sends a fax containing patient information to the wrong specialist, and the specialist calls the dental practice to say that he or she received the fax in error and destroyed it. The dental practice may be able to demonstrate, through its risk assessment, that there is a low probability that the patient information has been compromised.

The federal government has stated that events such as a hacker accessing an unencrypted database, and theft of unsecured patient information, would require breach notification under the new rule in almost all cases, just as they would have under the prior rule.

Breach log. Dental practices are required to keep a log of breaches involving fewer than 500 individuals, and submit the information annually to HHS (if a breach involves 500 or more, the dental practice must notify HHS when it notifies the individuals).[3] The prior rule required the annual report to include breaches that *occurred* during the preceding calendar year. The new rule requires annual reporting of breaches *discovered* during the prior calendar year. This change makes sense because a breach may not be discovered in the year that it occurred.

ACTION STEPS:

- ☐ ***Policies and procedures.*** Revise dental office breach notification policies and procedures to comply with the new rule (see Chapter 2, Step 22).
- ☐ ***Risk assessment form.*** Revise the risk assessment form that your practice uses to assess and document suspected breaches (see the sample form in Appendix 2.22.1).
- ☐ ***Breach log.*** Review the log that your dental practice uses for breaches involving fewer than 500 individuals and make sure the log records breaches that were *discovered* during the prior calendar year (not breaches that *occurred* during the year) (see sample form in Appendix 2.22.1).
- ☐ ***Training.*** Train staff to follow new breach notification procedures.
- ☐ ***Business associates.*** Make sure business associates understand the new rule and will comply when reporting breaches to the dental practice.
- ☐ ***Business associates.*** Make sure business associates understand the new rule and will comply when reporting breaches to the dental practice.
- ☐ ***Encryption.*** Since breach notification is not required for properly encrypted ("secured")[4] electronic patient information:
  - ☐ Determine which patient information is not properly encrypted, including information:
    - stored electronically (both on-site and off-site)
    - in transit
    - on mobile devices
  - ☐ Evaluate encryption options.
  - ☐ Implement reasonable encryption as appropriate.

[3] For information about reporting breaches to HHS, visit *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.*
[4] HHS has issued guidance on appropriate methods of securing PHI (see Chapter 2 Step 22).

C. Business Associates and Subcontractors

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 13.

Compliance Date: September 23, 2013, with a one-year transition period for certain business associate agreements that were in place prior to January 25, 2013.

Background: A dental practice's "business associates" are the outside persons or entities that perform services for the dental practice involving patient information. Examples of business associates include billing services, document storage companies, shredding and recycling firms, collection agencies and law firms, that have access to patient information. (For more information about who qualifies as a business associate, see "Who Are Your Business Associates?" in Chapter 2, Step 13.1). A dental practice must have a written agreement in place with each of its business associates. The agreement must contain certain provisions (see sample business associate agreement Appendix 2.13). A dental practice can take legal action if a business associate violates the agreement.

Prior rule: Under the prior rule, if a business associate or its subcontractor improperly used or disclosed patient information or violated the business associate agreement, the government could not impose penalties on the business associate or subcontractor.

New rule: The new rule requires business associates and their subcontractors to comply with many parts of HIPAA (including most of the Security Rule), and the government can directly impose penalties on business associates and subcontractors. A business associate or subcontractor is subject to government enforcement even if a written business associate agreement is not in place (note that if a business associate agreement is not in place between a dental practice and a business associate, the dental practice is not in compliance with HIPAA).

In addition, the new rule:

- changes the provisions that must be in the business associate agreement.
- clarifies that the "business associate" definition now also includes subcontractors, Patient Safety Organizations, Health Information Organizations, e-prescribing gateways, and other providers of data transmission services that require access to patient information on a routine basis. In addition, 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
- requires a business associate to have written agreements containing certain provisions in place with any of the business associate's subcontractors that will have access to patient information. A dental practice does not need to have agreements with its business associates' subcontractors — that is the business associates' responsibility.

New provisions in the business associate agreement. The 2013 Final Rule requires changes to business associate agreements. For example, the business associate agreement must now require the business associate to:

- comply, where applicable, with the HIPAA Security Rule with respect to electronic patient information.

- report to the dental practices breaches of unsecured patient information as required by the HIPAA Breach Notification Rule.
- ensure that subcontractors with access to patient information agree to the same restrictions that apply to the business associate.
- comply with the requirements of the HIPAA Privacy Rule that apply to the dental practice to the extent that the business associate is carrying out a HIPAA Privacy obligation of the dental practice.

Reporting business associate violations to HHS. Existing business associate agreements may state that the dental practice will report to HHS if the business associate is in material violation of the business associate agreement and the dental practice was unable to fix or stop the violation or terminate the agreement. Under the new rule, a dental practice can no longer report business associate violations to HHS.

Instead, a dental practice that is aware of a pattern or practice of the business associate in violation of the business associate agreement must take reasonable steps to fix or stop the violation, and, if those steps are not successful, the dental practice must terminate the agreement with the business associate if feasible. A business associate has a corresponding obligation with respect to its subcontractors, and subcontractors have a corresponding obligation with respect to their subcontractors.

Compliance dates for revising business associate agreements. New business associate agreements must comply with the new rules (see sample business associate agreement in Appendix 2.13). A dental practice must also update ***existing*** business associate agreements.

By September 23, 2013, any business associate agreement that was entered into on or after January 25, 2013 and that is still in effect must comply with the new rules.

Business associate agreements that were entered into before January 25, 2013 must be revised to comply with the new rules by the following dates:

- *September 23, 2013* if the agreement was modified or renewed between March 26, 2013 and September 23, 2013
- *The date such agreement is renewed or modified* if the agreement is renewed or modified on or after September 23, 2013 but before September 22, 2014
- *September 22, 2014* if the agreement was not modified or renewed between March 26, 2013 and September 22, 2014

Evergreen contracts: if a compliant business associate agreement was entered into on or before January 24, 2013, and it is not modified after that date, but it renews automatically without any change in terms, the dental practice and business associate must update the agreement by September 22, 2014.

Oral agreements. If a dental practice does not have a written business associate agreement in place with any business associate, the dental practice must enter into a compliant written agreement without delay.

Business associate "agents." A dental practice can be *directly liable* for the HIPAA violations of a business associate that is an "agent" of the dental practice (see Chapter 2, Step 13.3). Determining whether a business associate is an agent will be fact specific, taking into consideration the business associate agreement and extent of the dental practice's control. As with any business associate (agent or not), the dental practice must take reasonable steps to end any violation of HIPAA, and if that is not successful, the dental practice has to terminate the business associate agreement, if that is feasible (see Chapter 2, Step 13.2). The dental practice must also take steps to mitigate (lessen) harm resulting from the violation.

Due Diligence. Some business associates and subcontractors may already comply with their new HIPAA obligations. Others may not be aware of the HIPAA requirements, particularly if they are smaller organizations or have limited resources. HIPAA does not require "due diligence" when a dental practice selects a business associate, but proper due diligence can help a dental practice determine whether a business associate is likely to protect the dental practice's patient information. In some situations, a dental practice can be liable if a business associate violates HIPAA, so due diligence can also help protect the practice from liability. Here are some examples of how a business associate's conduct can result in liability or expense for the dental practice:

- A data breach is more likely if a business associate is not HIPAA compliant. When a business associate has a data breach, it is *the covered dental practice* that is required to send the notifications required under the Breach Notification Rule.
- A dental practice can be *directly liable* for HIPAA violations by a business associate that is an "agent" of the dental practice (see above and Chapter 2, Step 13.3).
- A dental practice is in violation of HIPAA if the dental practice is aware of a business associate's noncompliance and does not take certain steps (see Chapter 2, Step 13.2 "What if a business associate violates HIPAA or the business associate agreement?").

Examples of due diligence questions that a dental practice might ask business associates include:

- Did you know that business associates must comply with certain parts of HIPAA, including most of the Security Rule, and that the government can investigate and impose penalties on business associates that do not comply?
- Is your company HIPAA compliant?
- When did you perform your last security risk assessment?
- Are all of your workforce members trained to protect patient information?
- Has your company ever had a data breach? What happened? Did you tighten security afterward?
- Have you entered into business associate agreements with all of your subcontractors who have access to patient information?

"Certified" HIPAA compliant. What if a business associate is "certified"? It continues to be the case that certification does not guarantee compliance, and that "certified" persons and entities are still subject to enforcement by the federal government. The federal government has not established or endorsed a certification process for HIPAA compliance for business associates and subcontractors. 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.

ACTION STEPS:

- ☐ Make a list of all of the dental practice's business associates. Include all persons and entities, other than workforce members, that receive, create, maintain, transmit or otherwise have access to patient information. Include any Health Information Organizations, e-prescribing gateways, and individuals or entities that provide data transmission services and require routine access to patient information (see Chapter 2, Step 13.1, "Who are your dental practice's business associates?"). Include anyone that offers a personal health record on behalf of the dental practice, if applicable.
- ☐ Enter into a compliant business associate agreement, or update an existing agreement, by the applicable compliance date (see sample business associate agreement Appendix 2.13).
- ☐ If a business associate refuses to sign a business associate agreement or update an existing business associate agreement, the dental practice should try to correct the situation, and if not successful, the dental practice should terminate its relationship with the business associate. A dental practice can be subject to HIPAA penalties it if provides patient information to a business associate without a compliant business associate agreement in place.
- ☐ Make sure your business associates understand that (1) they must comply with HIPAA, (2) they must enter into HIPAA-compliant agreements with subcontractors that have access to patient information, and (3) business associates and subcontractors will be liable for failure to comply with applicable HIPAA provisions.

D. Restricted Disclosure to a Health Plan

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 14.5

Compliance Date: September 23, 2013.

Background: Under HIPAA, a patient has the right to ask a dental practice not to tell or give their patient information to a certain person or organization. In general, HIPAA does not require the dental practice to agree to the request. But if a dental practice does agree, it must honor the restriction until it is terminated, except in certain emergency situations.

In most cases, if a dental practice has agreed to a request for a restriction, the dental practice may terminate the restriction, but the dental practice must still apply the restriction to the patient information from before the date of termination. The patient can also terminate the restriction.

A dental practice must have procedures in place for accepting and considering patient requests for restrictions (Chapter 2, Step 14.5), and must document the requests that the dental practice agrees to. A dental practice may choose to document all requests whether or not the dental practice agrees to the restriction, although doing so is not required by HIPAA.

Prior Rule: Under the prior rule, if a patient asked a dental practice not to give information to the patient's health plan or dental plan, the dental practice was not required to agree. If the dental practice did agree to the request, the dental practice could terminate the restriction, but needed to continue to apply the restriction to patient information created or received before the termination.

New rule: Under the new rule, a dental practice ***must agree*** if a patient asks the dental practice not to give information to the patient's dental plan or medical plan, as long as the information:

- is for the purpose of carrying out payment or health care operations and is not otherwise required by law, *and*
- pertains solely to a health care item or service for which the patient or someone else (including a different plan) had paid the dental practice in full.

The dental practice cannot terminate such a restriction unless the patient agrees. A patient can agree to terminate this kind of restriction orally or in writing, but if the patient agrees orally the dental practice must document the oral agreement to terminate the restriction.

Telling or sending such restricted information to a health plan can be a HIPAA violation and subject to possible criminal penalties, civil monetary penalties, or corrective action. It may also require breach notification, and may need to be included in an accounting of disclosures.

Updating the Notice of Privacy Practices. A dental practice must update its Notice of Privacy Practices ("NPP") to include certain information about the new requirement (see Chapter 2, Step 3 and the sample NPP in Appendix 2.3.1).

Flagging the restricted information. A dental practice is not required to have separate or segregated records in order to make sure a patient's restriction request is honored. The dental practice must decide how best to flag restricted information to keep it from being disclosed to the plan. Dental practices should:

- ☐ Identify workforce members who need access to certain categories of patient information and train them to comply with the new requirements.
- ☐ Flag or make a notation in the records with respect to patient information that has been restricted so that such information is not inadvertently sent to or made accessible to a dental or medical plan.
- ☐ If any of the dental practice's business associates might disclose patient information to a plan, notify those business associates each time patient information has been restricted from disclosure to a plan.
- ☐ Prevent plans from accessing restricted patient information (e.g., during an audit) by using the dental practice's "minimum necessary" mechanisms, which should already be in place (Chapter 2, Step 5).

No obligation to notify patient's other health care providers. The new rule does not require the dental practice to inform other health care providers, such as dental labs, specialists or pharmacies, that the patient has restricted disclosure to a health plan. It is the patient's obligation to request restrictions from other providers. Dental practices may counsel patients that the restriction won't apply to other providers unless the patient requests a restriction from them, too, and they are paid in full.

A dental practice can use paper prescriptions rather than electronic prescribing to help a patient who requested a restriction to a plan. That way, the patient will have time to request a restriction at the pharmacy and pay the pharmacy out of pocket before the pharmacy submits a bill to the health plan. With electronic prescriptions, pharmacies sometimes bill the plan before the patient arrives to pick up the prescription.

Business associates. If a dental practice has any business associates that disclose patient information to dental or medical plans, the dental practice should make sure they understand the new requirement, and notify them each time a patient restricts disclosures to a plan.

Source of the payment in full. A dental practice must be paid in full if the patient wishes to restrict disclosure to a plan. Payment can be made by the patient or by someone else for the patient, including another medical or dental plan.

Dishonored payment. If a patient tries to pay in full but the payment is dishonored, the dental practice must not contact the plan before making a reasonable effort to contact the individual to obtain payment, in accordance with the dental practice's usual procedures for asking patients for a different form of payment. However, the dental practice does not need to place the patient's debt in collection before billing the health plan. ***To avoid this situation, the dental practice may require payment in full at the time a patient asks for a restriction.***

Precertification. If a patient asks for a restriction on disclosures to a plan for an item or service, and the plan would require precertification for that item or service, the dental practice may require the patient to pay in full before the dental practice provides the item or service, in order to avoid a situation where the patient's payment is dishonored and the dental practice can't be reimbursed either by the patient or by the plan.

If dental care has already been started. If a patient asks for a restriction to a plan after the dental care has been started, the dental practice may not be able to restrict the information. For example, information about the care may already have been disclosed to the plan.

Follow-up care. When a patient asks the dental practice not to give information to a plan, the dental practice should talk to the patient about what will happen if the patient needs follow up care. If the patient:

- doesn't ask for an additional restriction for the follow up care, and
- does not pay in full for the follow up care,

and the plan needs the restricted information to determine whether the follow up care is medically necessary or appropriate, then the dental practice is permitted give the restricted information to the plan. The dental practice must only give the plan the minimum necessary amount of restricted information (Chapter 2, Step 5). The patient does not need to sign an authorization form before the dental practice gives the plan information in this situation, because the dental practice is giving the information to the plan for payment purposes.

Restriction only applies to the plan. A dental practice that agrees not to give a patient's information to a dental or medical plan may still make appropriate disclosures to persons and companies other than the plan. For example, the dental practice can give the information to a collection agency if necessary. The dental practice can also give the information if required by law — for example, to respond to a court order or subpoena.

FSAs and HSAs. A patient may use a Flexible Spending Account ("FSA") or a Health Savings Account ("HSA") to pay in full when the patient asks a dental practice not to give information to a health plan, but the patient may not request a restriction on disclosures to the FSA or HSA if the disclosure is necessary for that payment.

Disclosures to the health plan's business associates. A dental practice may not disclose restricted information to the health plan itself or to a business associate of the health plan. However, the dental practice may disclose the restricted information to its own business associates, as appropriate.

If Medicare or Medicaid requires the dental practice to include the restricted information in a required audit. HIPAA allows a dental practice to disclose patient information when required by law, even when a restriction is in place. Medicare conditions of participation are required by law. If a dental practice is required by law to submit patient information to a federal health plan like Medicare, the dental practice may do so as necessary to comply with that legal requirement.

If state law, Medicare, or Medicaid prevents a dental practice from billing the patient and receiving cash payment from the patient over and above permissible cost sharing amounts. If a dental practice is required by state or other law to submit a claim to a health plan for a covered service, and there is no exception or procedure for patients who wish to pay out of pocket for the service, then giving the plan the information is required by law and the dental practice may give the information to the plan.

However, Medicare, for example, may permit a patient to refuse, of his or her own free will, to authorize the submission of a bill to Medicare. In that case, the dental practice is not required to submit a claim to Medicare for the covered service and may accept an out of pocket payment. The Medicare limits on what the dental practice may collect from the patient would continue to apply to the dental practice's charge for the covered service. Under these circumstances, if a patient who is on Medicare asks a dental practice not to give Medicare information about a covered item or service, and the patient pays out of pocket, HIPAA requires the dental practice not to give the information to Medicare.

Requests to restrict only part of the information about a single appointment. If a dental practice provides several items or services in a single appointment, and the patient asks the dental practice not to give the plan information about a portion of the appointment, the dental practice may be prohibited from unbundling the services, or it may be more costly to unbundle the services. In such cases, the dental practice should counsel patients about the practice's ability to unbundle and the impact of doing so (e.g., the plan may still be able to determine that the restricted item or service was performed).

If the dental practice can unbundle to accommodate the request, it should do so. If the dental practice cannot unbundle, it should:

- inform the patient, and
- give the patient the opportunity to restrict and pay out of pocket for the entire bundle of items or services.

HMOs. A dental practice in an HMO should abide by a request to restrict disclosure to a health plan unless doing so would be inconsistent with state or other law. If a patient requests a restriction and the dental practice is prohibited by law from accepting payment from a patient above the cost-sharing amount, the dental practice may counsel the patient that he or she will have to use an out-of-network provider for the item or service in order to restrict disclosure to the HMO. If a dental practice in an HMO is able under law to treat the services as out-of-network services, it should do so in order to comply with the requested restriction.

A contractual requirement to submit a claim or otherwise disclose information to an HMO does not exempt a dental practice from the HIPAA obligations to agree to a request to restrict disclosure to a health plan for items or services paid for in full. Dental practices should review their HMO and managed care agreements.

Disclosures required by law. If the dental practice is required by law to tell or send the information to the plan, the dental practice may do so.

ACTION STEPS:

- ☐ Review the dental practice's procedures for accepting, considering, and documenting patient requests for restrictions on disclosure of their information (Chapter 2, Step 14.5).
- ☐ Update the procedures to require the dental practice to agree, as appropriate, to a request to restrict disclosure to a health plan for health care items and services for which the dental practice has been paid in full (Chapter 2, Step 14.5).
- ☐ Develop and implement procedures to flag or make a notation in the records when information has been restricted so that such information is not inadvertently sent to or made accessible to a health plan.
- ☐ Train staff to comply with the new procedures.
- ☐ Identify business associates that may disclose patient information to plans. Make sure they understand the new rule, and notify them of all patient information that has been restricted from disclosure to a plan.
- ☐ Update the Notice of Privacy Practices (see Appendix 2.3.1).
- ☐ Review any HMO and managed care agreements and applicable law to determine how to comply with requests for restrictions on disclosures to health plans.

E. Patient Request to See and Get Copies of Records ("Access")

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section:
Chapter 2, Step 14.1

Compliance Date: September 23, 2013.

Background. With certain limitations, HIPAA gives patients the right to see and to get copies of their patient information that is in a "designated record set" (Chapter 2, Step 4). A dental practice must respond to requests within the timeframe required by HIPAA. A dental practice is permitted (but not required) to charge certain limited fees for copies.

1. TIMEFRAME FOR ACTION

Prior rule. Under the prior rule, a dental practice had to act on a request within 30 days (60 days if the information was off-site). The dental practice could get one 30-day extension.

New rule. The new rule requires a dental practice to act on a request within 30 days whether the information is maintained onsite or offsite. The 30-day timeframe applies whether the dental practice maintains the designated record set on paper or electronically. The 30-day period begins to run when the dental practice receives the request. Time spent agreeing on the electronic format, etc., does not delay the start of the 30-day period.

ACTION STEPS:

- ☐ Update your policies and procedures for responding to requests for access (to see or get copies of patient information) so that the dental practice will respond to requests within 30 days whether the patient information is stored on-site or off-site. The practice may still request one 30-day extension by providing a written statement of the reasons for the delay and the date by which the dental practice will complete its action on the request.

2. PATIENT REQUESTS FOR COPIES OF ELECTRONIC RECORDS

Prior rule. Under the prior rule, a dental practice had to allow patients to get copies of their patient information in the form or format that the patients requested, if the information was readily producible that way. If the information was not readily producible in the form or format the patient asked for, the dental practice could provide a readable hard copy.

New rule. If a patient asks for an *electronic copy* of his or her patient information, and the dental practice maintains that information in an *electronic* designated record set, the dental practice must provide the copy in the electronic form and format requested by the patient, if it is "readily producible" that way.[5] If it is not readily producible in the form and format that the patient asked for, the dental practice must provide the information in the readable

[5] For example, if a patient asked for a copy via a web-based portal, but the only format available on the dental practice's system was a PDF, HIPAA only requires the dental practice to provide the PDF.

electronic form and format that the patient and the dental practice agree upon. But if the patient will not agree to any of the electronic forms and formats that the dental practice can readily produce, the dental practice must provide a hard copy as an option. The new rule is not limited to patient information in an electronic dental record; the rule applies to all patient information in an electronic designated record set (see Chapter 2, Step 4).

Paper records. If a patient asks for a copy of information that the dental practice has in a paper designated record set, HIPAA still permits the dental practice to provide the patient with a paper copy. HIPAA does not require a dental practice to use electronic records. If a patient asks for an electronic copy of a paper record, the dental practice may scan it and provide it electronically, but the dental practice is not required to do so. A dental practice is only required to provide electronic copies of records that the dental practice maintains electronically.

Electronic records. If a dental practice has an electronic designated record set, the dental practice must be able to provide an electronic copy of that information within the required timeframe (see section 2.E.1 above). If the electronic technology is capable of producing a paper copy but not an electronic copy, a dental practice could, for example, print a paper copy, scan the copy, and provide the patient with an electronic copy of the scanned information.

Electronic media. If a patient brings his or her own electronic media, such as a CD-ROM or USB drive, to the dental practice and asks the dental practice to use the media to provide an electronic copy, the dental practice may refuse as long as the dental practice has done a written risk analysis and determined that using outside electronic media poses an unacceptable level of risk. A dental practice may have a supply of new electronic media on hand to use to provide electronic copies to patients. The dental practice may provide the media free of charge, or factor the cost of the electronic media into the reasonable, cost-based fee that it can charge the patient for the copy (see "Fees" in section 2.E.3 below).

Email. A dental practice may send a patient an electronic copy in an unencrypted email *if the practice has advised the patient of the risk* and the patient still prefers to receive the information in an unencrypted email. If the patient has been notified of the risk and still prefers unencrypted email, the patient has the right to receive the unencrypted electronic copy in an email. Notification of the risk can be included in the dental practice's form for requesting copies of patient records (see *Sample Request for Access*, Appendix 2.14.1). The dental practice must implement reasonable safeguards, including reasonable procedures to ensure that the dental practice correctly enters the email address. However, the dental practice is not responsible for the email while in transit, nor once it is delivered to the patient.

Requests to provide electronic copies to someone else. If a patient asks the dental practice to send a copy of the patient information to someone else, the dental practice must do so, whether the dental practice maintains the designated record set electronically or on paper. The request must be in writing, signed by the patient, and must clearly identify the person who will receive the copy and where to send the copy.

Direct access to systems not required. A dental practice is not required to provide patients with direct access to the dental practice's systems.

Business associates. If a dental practice's business associate has patient information in a designated record set, the patient has the right to see and get copies of the information. The business associate agreement should say whether the business associate will provide patients with access to information about them, or whether the dental practice will provide this access with the business associate's support. For example, the business associate agreement may require the business associate to give copies of requested information directly to the patient, or to the dental practice, which will in turn provide the information to the patient.

ACTION STEPS:

- ☐ **List of designated record sets.** Understand which record sets are electronic and determine what electronic copy forms and formats are readily producible for each electronic designated record set. ***If an electronic designated record set is unable to produce at least one form and format of electronic copy, upgrade the technology so that at least one form and format is readily producible.***
- ☐ **Outside electronic media.** If you have not already done so as part of your HIPAA Security Rule compliance, conduct a written risk assessment to determine whether using outside electronic media poses an unacceptable level of risk (e.g., viruses, malware). If your risk assessment determines that the level of risk is unacceptable, the dental practice may refuse to permit electronic copies to be downloaded onto outside media.
- ☐ **Practice-supplied electronic media.** Have a supply of new electronic media on hand for the dental practice's use in providing electronic copies, either without charge or for an appropriate reasonable, cost-based fee (see 2.E.3 below).
- ☐ **Request form.** Update or develop appropriate written request forms that the dental practice will require patients to fill out when they want to see or get copies of their records (Chapter 2, Step 14.1 and Appendix 2.14.1). If a patient asks for a copy to be sent to someone else, the request must be in writing and contain certain information.
- ☐ **Policies and procedures.** Review your policies and procedures for responding to patient requests to see and get copies of their records. Update as necessary to comply with the new rule. See sample policies and procedures in Chapter 2, Step 14.1.
- ☐ **Training.** Train staff to respond appropriately to patients' requests to see or get copies of their information. Training should include any new procedures and forms, including procedures for emailing information to patients.

3. FEES FOR COPIES

Background: HIPAA does not require a dental practice to charge patients for providing copies of their patient information, but if a dental practice charges for copies the dental practice may only charge a reasonable, cost-based fee.

Prior rule. The prior rule did not specifically address permissible fees for electronic copies.

New Rule. The new rule adds requirements for charging reasonable, cost-based fees for electronic copies.

Electronic copies. A dental practice that provides an electronic copy may charge a reasonable, cost-based fee, and the fee can include certain costs associated with labor and supplies for creating an electronic copy, including the cost of electronic media (for example, a blank CD-ROM or USB drive) if the patient agrees to receive the copy on electronic media supplied by the dental office. The dental practice may charge for postage if the patient requests that the electronic media be sent via U.S. mail or by courier. However, the dental practice may not include fees associated with maintaining systems, retrieval costs, or infrastructure costs in the fee charged for electronic copies.

Labor for copying and supplies. The fee may include the labor for copying the information, whether in paper or electronic form, but not the labor cost of retrieving the information. The fee may also include supplies for creating a paper copy, or for providing a copy on electronic media (e.g., CD-ROM or USB drive) if the patient agrees to use the dental practice's media. Labor costs may include skilled technical staff time spent to create and copy an electronic file, such as compiling, extracting, scanning and burning the information to electronic media, and distributing the media. Labor costs may also include the time spent preparing an explanation or summary of the information, if appropriate.

Cost of new technology. The cost of obtaining new technologies is not a permissible fee to include in the supply costs.

Postage. The dental practice may charge for postage if the patient asks the dental practice to send electronic media or paper copies through the U.S. mail or via courier, whether to the patient or to someone else.

Maintaining systems or recouping capital. Reasonable cost-based fees do not include fees associated with maintaining systems or recouping capital for data access, storage or infrastructure.

Retrieval fee. The dental practice may not charge any kind of retrieval fee for electronic or paper copies. This applies to both standard retrieval fees and to retrieval fees based on retrieval costs.

State law limits. State law may limit the fees that a dental practice may charge for providing patients with copies of their records. If so, the state limit is relevant in determining whether a dental practice's fee is "reasonable" under HIPAA. For example, if a state permits a charge of 25 cents per page, but the dental practice is able to provide an electronic copy at a cost of five cents per page, the dental practice may not charge more than five cents per page (since that is the "reasonable" and "cost-based" amount). However, if the dental practice's cost is 30 cents per page but the state law limit is 25 cents per page, the dental practice may not charge more than 25 cents per page (since charging 30 cents per page would be the "cost-based amount," but would not be "reasonable" in light of the state law).

ACTION STEPS:

- ☐ **Fees.** Determine whether your dental practice will charge a fee for providing copies of patient information.
- ☐ **If your dental practice will charge a fee,** determine the fees that are permissible under HIPAA and applicable state law. Develop an appropriate fee schedule for electronic and paper copies.

F. Subsidized Marketing Communications

Applies to: Any covered entity dental practice that receives payment for making a "marketing communication."

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 10

Compliance Date: September 23, 2013.

Background: A "marketing communication" is a communication that encourages someone to buy a product or service. For example, a marketing communication could be a brochure for a new product or service. A marketing communication may be transmitted via U.S. mail, email, fax, or over the phone.

In many cases, HIPAA requires a dental practice to have a patient sign an authorization form before the dental practice (or a business associate) makes a marketing communication to the patient, whether the communication encourages the patient to buy a product or service offered by the dental practice or by a third party. However, a dental practice does not need to have the patient sign an authorization form before the dental practice encourages the patient to buy a product or service in a face-to-face, in person communication, or before the dental practice gives the patient promotional gifts of nominal value.[6]

Prior rule: The prior rule did not require patient authorization if a dental practice made a communication describing its own health-related product or service, or used or disclosed patient information for treatment of a patient or for case management or care coordination for the patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the patient, provided the use or disclosure was permitted by HIPAA. The authorization requirement under the prior rule depended in part on whether a marketing communication was for treatment purposes or for health care operations.

New rule: Under the new rule, if a dental practice (or its business associate) receives "financial remuneration" (dollars) for making a marketing communication from a third party whose product or service is being marketed, or by someone else on the third party's behalf, the dental practice is required to have a patient sign an authorization form if the dental practice will use patient information in order to make the marketing communication (e.g., patient names and addresses, or information about a patient's dental condition).

For example, if a toothpaste manufacturer pays a dental practice to mail an advertisement for the manufacturer's new toothpaste to all (or some) of the practice's patients, the practice is in violation of HIPAA if it sends the advertisement to patients who have not signed an appropriate authorization form. Patients are not required to sign an authorization form if the manufacturer provides the advertisements to the dental practice free of charge but does not pay the dental practice money for sending the advertisements to the patient for a permissible purpose under HIPAA (examples of permissible purposes include treatment, case management, care coordination, or health plan benefits), because the authorization is only required if the dental practice receives *financial remuneration* (dollars) for making the communication, not nonfinancial or in-kind remuneration.

[6] For example, dentists may give patients free toothbrushes, floss and toothpaste without having the patients sign an authorization form. Other examples of promotional gifts of nominal value that may be distributed without the patient's prior authorization include product samples, and pens, notepads, calendars and cups that are embossed with a logo or that display the name of a product or provider.

The authorization form must state that the dental practice received payment for the making the communication. The new rule does not apply if the dentist receives nonfinancial or in-kind remuneration for making the communication if the communication is for a permissible purpose under HIPAA. Unlike the prior rule, the new rule on "subsidized" (paid) marketing communications applies whether a communication is related to "treatment" or "health care operations."

Under the new rule, disclosures of patient information to a third party for the third party's marketing purposes is covered under "sale of patient information" rather than under "marketing." If a dental practice receives a payment or anything of value (financial, nonfinancial, or in-kind) for *disclosing* patient information, it is considered a "sale of patient information" and not a "subsidized marketing communication" and separate HIPAA provisions apply. (see Chapter 1.G and Chapter 2, Step 11).

Examples:

Subsidized marketing communication: A third party pays a dental practice to send patients a marketing message about the third party's product or service.

Sale of patient information: A dental practice receives something of value for giving patient names and addresses to a company so that the company can send the patients information about the company's product.

Note that a subsidized marketing communication requires authorization if the dental practice receives *payment*, but that the sale of patient information authorization requirement applies if the dental practice receives *anything of value* (for example, financial, nonfinancial, or in-kind remuneration).

An authorization form for marketing communications may apply to a single product or service or the products or services of one third party, or it may apply broadly to subsidized communications generally as long as the form adequately describes the intended purposes of the requested uses and disclosures, states that the dental practice will receive remuneration for making the communication(s), and meets the requirements for a HIPAA authorization form (Chapter 2, Step 9). For example, the form must state that the patient may revoke the authorization at any time if the patient wishes to stop receiving the marketing communications. Sample authorization forms for marketing communications are at Appendices 2.10.

Rather than asking patients to sign the necessary authorization forms, a dental practice may simply decide never to accept payment for making marketing communications except for:

- face-to-face communications.
- promotional gifts of nominal value.
- marketing communications made for nonfinancial or in-kind remuneration, or for no remuneration.

The new rule on subsidized marketing communications does not change the exception for face-to-face communications and promotional gifts of nominal value, so a dental practice does not need to have a patient sign an authorization form before the dental practice makes a face-to-face communication or provides a promotional gift of nominal value, even if the dental practice received payment from a third party. However, communications made over the phone, through the mail, or via email do not constitute face-to-face communications, and would require an authorization form from the patient if the dental practice is paid for making the communication.

The new rule also creates an exception for sending certain refill reminders or communications about a drug or biologic, as long as:

- the drug or biologic is currently being prescribed for the patient, and
- any payment received by the dental practice in exchange for making the communication is reasonably related to the dental practice's cost of making the communication (i.e., it covers only the costs of labor, supplies and postage to make the communication, and does not generate a profit or include payment of other costs).

Payment ("financial remuneration"). A dental practice only needs to have patients sign authorization forms if the dental practice (or its business associate) receives "financial remuneration" (financial payment) for making the communication. Nonfinancial or in-kind remuneration does not require patient authorization. For example, if a third party provides a dental practice with materials describing the third party's product or service, and the communication to the patient is for a permissible purpose under HIPAA, the dental practice may provide the materials to patients without first obtaining the patients' written authorization.

Financial remuneration for other purposes. If the payment that the dental practice receives is not for the purpose of making the marketing communication, but instead is for another permissible purpose, then the patient's written authorization is not required. For example, if a third party pays a dental practice to implement a disease management program, the dental practice could provide patients with communications about the program without prior authorization as long as the communications are about the dental practice's program itself. The communications would only be encouraging people to participate in the dental practice's disease management program and would not be encouraging people to use or buy the business' product or service.

Treatment-related communications. The dental practice must get the patient's written authorization before the dental practice makes the communication if the dental practice receives payment in exchange for making one of the following kinds of marketing communications:

- A marketing communication for treatment of a patient by a health care provider, including case management or care coordination for the patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
- A marketing communication for case management or care coordination, contacting of patients with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

If the dental practice does not receive payment in exchange for making such a communication, then the dental practice does not need to get the patient's authorization.

Business associates. If a dental practice would need to get a patient's written authorization before making a certain marketing communication, then authorization is also required:

- if the dental practice's business associate sends the communication on behalf of the dental practice, or
- if a business associate receives the payment from the third party in exchange for the marketing communication (whether the communication is made by the dental practice, by the business associate, or by someone else on behalf of the dental practice).

Communications promoting health in general. Communications that do not promote a product or service from a particular provider, but rather promote health in general, such as promoting a healthy diet or encouraging patients to get certain routine diagnostic tests, do not constitute marketing and do not require patients to sign an authorization form.

Communications about government programs. A dental practice may use and disclose patient information to communicate with patients about eligibility for programs such as Medicare, Medicaid or CHIP without having the patients sign authorization forms.

G. Sale of Patient Information

Applies to: Any covered entity dental practice that intends to exchange patient information for payment or anything else of value (including financial, nonfinancial and in-kind remuneration).

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section:
Chapter 2, Step 11

Compliance Date: September 23, 2013.

Background: HIPAA restricts the way dental practices can use or disclose patient information, including "demographic" information such as names, addresses, ages, genders, etc.

Prior rule: Under the prior rule, a dental practice could not sell patient information, but HIPAA did not prohibit a dental practice from receiving remuneration for an otherwise permitted disclosure of patient information.

New rule: Under the new rule, even if a disclosure is permitted by HIPAA, a dental practice cannot exchange the patient information for remuneration from or on behalf of the recipient of the information without a signed authorization from a patient that states that the dental practice will be remunerated for the disclosure. The new rule applies whether the remuneration is direct or indirect, and whether the remuneration is financial (the new rule also applies if the remuneration is nonfinancial or in-kind). There are certain exceptions to the authorization requirement (examples are discussed below).

"Sale" of patient information. Even though the 2013 Final Rule refers to a "sale," it doesn't matter whether there is a change of "ownership" of the patient information. For example, a "sale" could involve a lease, license, etc., or even just a disclosure of patient information in exchange for "remuneration" (payment or anything else of value).

Exceptions. There are several exceptions to the definition of a "sale" of patient information, including certain disclosures for certain public health, research, treatment and payment purposes. Examples of other exceptions include:

- ***Sale of the practice.*** A dental practice that discloses patient information in connection with the sale of the practice to another HIPAA covered entity (or to a buyer that will become a covered entity after the sale), or for related due diligence.
- ***Disclosure of patient information that is required by law,*** such as when a dental practice must disclose patient information in response to a court order or subpoena.
- ***Permitted reasonable, cost-based fee.*** A disclosure of patient information for a reasonable, cost-based fee to cover the cost to prepare and transmit the patient information, or for a fee permitted by other law, if the disclosure is permitted by HIPAA. For example, it is not a "sale" of patient information when a patient asks the dental practice to send a copy of his or her information to a designated third party, and the dental practice charges the patient a reasonable, cost-based fee for the copies as permitted by HIPAA (Chapter 2, Step 14.1).
- ***HIE fees.*** If a dental practice pays a fee to participate in a health information exchange ("HIE") and exchanges patient information as appropriate through the HIE, the payment is for the services provided by the HIE and not for the data itself.
- Disclosures of patient information for payment collection activities.

De-identified patient information. Remember, if patient information is properly "de-identified,"[7] the information is no longer protected by HIPAA. Therefore, exchanging de-identified information for remuneration is not a "sale" of patient information.

[7] To de-identify patient information, 18 specific "identifiers," such as name, address, Social Security number, and other information, must be removed from the information, and the dental practice must have no knowledge that the information could be used, alone or in combination with other information, to identify the patient. For information about de-identification, see Chapter 2, Step 21.

H. Decedents

1. PATIENTS WHO HAVE BEEN DECEASED MORE THAN 50 YEARS

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 8.

Compliance Date: September 23, 2013.

Prior rule: Under the prior rule, HIPAA applied to information about a deceased patient no matter how long the person had been deceased.

New rule: Under the new rule, HIPAA no longer applies to information about a patient who has been deceased for 50 years.

Disclosure not required after 50 years. A dental practice entity may choose to protect a deceased patient's information for longer than 50 years. HIPAA does not require the use or disclosure of information about a patient after 50 years has passed from the date of death.

Not a record retention period. The 50-year period is not a record retention requirement. In general, state law determines how long patient records must be retained.

State law may provide longer period. Laws other than HIPAA, such as state law, may provide a greater period of protection. HIPAA does not preempt state law that is contrary to HIPAA if the state law provides greater protection to the patient.

Must know date of death. A dental practice must know the date of death in order to disclose information about a patient who has been deceased 50 or more years. The dental practice cannot use the last date in the dental record to determine whether a decedent's information may be used or disclosed.

Other HIPAA provisions. Other HIPAA provisions pertaining to deceased patients remain unchanged, such as disclosures to coroners, medical examiners and funeral directors, disclosures for tissue donation purposes, and disclosures for certain research projects.

2. FAMILY MEMBERS AND OTHERS

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 8.3

Compliance Date: September 23, 2013.

Prior rule: Under the prior rule, a dental practice had to get an authorization form signed by a deceased patient's "personal representative" before disclosing information about the deceased patient to family members or others who were involved in the patient's care or payment for care, unless state law permitted a disclosure to another family member, such as a surviving spouse.[8]

[8] Such a state law would be considered "more stringent" than HIPAA. If there is a conflict between HIPAA and a more stringent state law, the dental practice must comply with the state law.

New rule: The new rule permits a dental practice to disclose certain information about a deceased patient to family members[9] and others who were involved in the patient's care or payment for care without first getting the written authorization of the personal representative. For example, a dental practice could disclose billing information to a family member of a deceased patient who is helping wrap up the patient's estate.

However, if the dental practice knows that the patient had "expressed a preference to the contrary," then the dental practice must first get the written authorization of the patient's personal representative before making the disclosure.

Disclosure to family and others not required. The new rule *permits* a dental practice to make such disclosures — the rule does not *require* a dental practice to do so. For example, if a dental practice believes such a disclosure would not be appropriate, the dental practice is not required to make the disclosure.

Reasonable assurance. A dental practice may request reasonable assurance that the person requesting information about a deceased patient is a family member or was involved in the deceased patient's care or payment for care. (Chapter 2, Step 6)

Limit disclosures. Dental practices generally should not share information about past, unrelated medical problems under this provision.

Authority of personal representative. The new provision does not change the authority of a deceased patient's personal representative.

Limitation on "others involved in care or payment for care." This provision does not generally apply to health care providers, health plans, public health authorities, law enforcement officials, and others whose access to patient information is governed by other HIPAA provisions.

Caution: The new rule does not provide guidance about when a dental practice is expected to know that a patient has expressed a preference that information not be disclosed to a family member or other person, or how that differs from a request for restricted disclosure (Chapter 2, Step 14.5). Dental practices may wish to proceed cautiously until further clarification is available from HHS.

ADA® TIP

A dental practice may find it simpler to require written authorization from a deceased patient's personal representative for disclosures about deceased patients, even to family members and others who were involved in a deceased patient's care or payment for care.

Decision tree: Appendix 2.8 provides a sample decision tree tool to help understand the new rules related to decedents.

[9] HIPAA defines "family member" to include a patient's:
- Dependents, which means "any individual who is or may become eligible for coverage under the terms of a group health plan because of a relationship to a participant", and
- Relatives. The following relatives of the patient by marriage, adoption, or blood (blood relatives include partial blood relatives, such as half-siblings):
  - The patient's parents, spouses, siblings, and children.
  - Grandparents, grandchildren, aunts, uncles, nephews, and nieces.
  - Great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
  - Great-great grandparents, great-great grandchildren, and children of first cousins.

ACTION STEPS:

- ☐ Determine whether the dental practice will:
  - ☐ ***Option 1 – Require authorization.*** Require written authorization from a deceased patient's personal representative for a disclosure to a family member and other persons who were involved in the deceased patient's care or payment for care, ***or***
  - ☐ ***Option 2 – Permit disclosure.*** Permit a disclosure of a deceased patient's information to family members and others who were involved in the patient's care or payment for care (the dental practice should request proof of patient death and familial relation in such cases).
- ☐ ***If permitting disclosure,*** be aware that the dental practice must get written authorization of the patient's personal representative before making a disclosure if a patient expressed a preference that the disclosure not be made.
- ☐ ***Train staff.*** Whether the dental practice should train appropriate staff members to respond appropriately to requests for information about deceased patients.

I. Enforcement

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 1, Section 1

Effective date: March 26, 2013

Background: The Office for Civil Rights ("OCR"), an agency of HHS, enforces HIPAA. OCR has the right to investigate complaints and suspected violations and to impose civil money penalties on dental practices that violate HIPAA. Some HIPAA violations also carry criminal penalties.

Generally, when OCR receives a complaint about a dental practice's HIPAA compliance, it conducts a preliminary review. If the review indicates a possible HIPAA violation, OCR may proceed with an investigation. If OCR learns of an alleged HIPAA violation (for example, from a state or federal agency, breach notification report, or in the news), OCR has the right to investigate.

Prior rule: Under the prior rule, OCR had discretion as to whether to investigate.

New rule: Under the Final Rule, OCR will formally investigate if a preliminary review indicates a violation due to willful neglect. If OCR finds a violation due to willful neglect, it will very likely impose civil money penalties. If the facts indicate a degree of culpability less than willful neglect, OCR has discretion as to whether or not to investigate.

Prior rule: The prior rule required OCR to try to resolve investigation reviews by informal means.

New rule: OCR is no longer required to attempt to resolve investigations or compliance reviews by informal means. OCR may move directly to a civil money penalty without exhausting informal resolution efforts, particularly in cases involving willful neglect violations.

Coordinating enforcement with other agencies. The new rule also expands OCR's ability to share patient information in order to coordinate with other law enforcement agencies, such as state attorneys general and the Federal Trade Commission.

Enforcement of other HIPAA rules. The enforcement regulations relate to compliance with the HIPAA Privacy, Security, and Breach Notification Rules, as well as other HIPAA Administrative Simplification regulations such as the standards for:

- Electronic Transactions and Code Sets Rule(s).
- Standard Unique Employer Identifier (EIN) Rule.
- Standard Unique Health Identifier for Health Care Providers (NPI Rule).

J. Penalties

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 1, Section 1.

Effective Date: The increased penalties apply to HIPAA violations occurring on or after February 18, 2009.

Background: OCR has the right to impose civil money penalties on dental practices that violate HIPAA. Some HIPAA violations carry criminal penalties, including fines and imprisonment. OCR also has the authority to require a dental practice to take corrective action, including instigating a formal (and costly) Corrective Action Plan if OCR finds the dental practice noncompliant.

Prior rule. Under the prior rule, civil money penalties for dental practices that did not comply with HIPAA were limited to $100 or less per violation, up to an annual cap of $25,000 for all violations of the same HIPAA requirement or prohibition.

New rule. The new rule has tiered penalty amounts for increasing levels of culpability, up to an annual cap of $1.5 million for all violations of the same HIPAA requirement or prohibition. If a violation was due to willful neglect and was not corrected within 30 days, there is a *minimum* penalty of $50,000 per violation.

Violation Category	Penalty Range Per Violation	Maximum Penalty for All Such Violations of Identical Provisions in a Calendar Year
Did not know[10]	$100 - $50,000	$1.5 million
Reasonable cause[11]	$1,000 - $50,000	$1.5 million
Willful neglect, timely corrected[12]	$10,000 - $50,000	$1.5 million
Willful neglect, not timely corrected[13]	$50,000	$1.5 million

How violations are counted. 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. For instance, usually with a breach of unsecured patient information there will be both (1) an impermissible use or disclosure and (2) a safeguards violation, and OCR may calculate a separate civil money penalty for each. As such, a dental practice may be liable for multiple violations of multiple requirements, up to a cap of $1.5 million for each requirement.

[10] For a violation where it is established that the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, that such person violated such provision.
[11] For a violation in which it is established that the violation was due to reasonable cause and not due to willful neglect.
[12] For a violation in which it is established that the violation was due to willful neglect and the violation was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred.
[13] For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or by exercising reasonable diligence, would have known that the violation occurred.

Aggravating and mitigating factors. HIPAA contains a list of aggravating and mitigating factors that can affect the amount of a civil money penalty. The prior rule gave the government discretion as to whether and how to apply the factors when determining the amount of a penalty for a HIPAA violation. The new rule requires the government to consider the factors when determining the amount of a penalty for a HIPAA violation.

The maximum penalty amount will not be imposed in most cases. The OCR will determine the amount of a penalty on a case-by-case basis, depending on the nature and extent of the violation and the nature and extent of the resulting harm, as well as other aggravating and mitigating factors listed in 45 CFR 160.408. Examples of the factors include:

- the number of individuals affected.
- whether the violation caused physical, financial, or reputational harm or hindered a patient's ability to obtain health care.
- the dental practice's history of prior compliance or noncompliance.
- the financial condition of the dental practice.
- whether the imposition of a civil money penalty would jeopardize the dental practice's ability to continue to provide health care.
- the size of the dental practice.

OCR may waive a penalty in whole or in part to the extent that payment would be excessive relative to the violation, and OCR has the discretion to settle any issue or case or to compromise the amount of civil money penalty assessed for a HIPAA violation.

K. Fundraising

Applies to: All covered entity dental practices that wish to use information about patients in connection with a fundraising campaign for the dental practice (for example, by sending fundraising communications to patients). This provision does not apply when a dental practice uses only a public directory to send fundraising communications to everyone in a geographic area.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 24

Compliance date: September 23, 2013.

Background: Although most dental practices do not conduct fundraising campaigns to raise funds for the practice, HIPAA has rules that apply when patient information is used in connection with such a fundraising campaign.

Prior rule: The prior rule required dental practices who were conducting fundraising campaigns to give people the opportunity to opt out of receiving future fundraising communications. A dental practice was required to make reasonable efforts to ensure that people who decide to opt out of receiving future fundraising communications were not sent such communications.

New rule: The new rule strengthens the opt-out requirement and makes it a HIPAA violation to send a fundraising communication to someone who has opted out. Only certain patient information may be used for fundraising. Clear and conspicuous information about how to opt out must be included in each fundraising communication. The opt-out process must not create an undue burden on the patient or cost more than a nominal amount. Only limited patient information may be used in connection with fundraising communications. If a dental practice intends to use patient information for fundraising, the Notice of Privacy Practices must contain certain required information. Finally, the dental practice cannot condition treatment or payment on the patient's choice to receive fundraising communications.

Definition of fundraising communication. A "fundraising communication" is defined as a communication to a person by any means (e.g., U.S. mail, email, telephone, etc.) made for the purpose of raising funds for the dental practice, whether the communication is made by:

- the dental practice
- a business associate on behalf of the dental practice, or
- a foundation related institutionally to the dental practice.

Notice of Privacy Practices. If a dental practice intends to use patient information for fundraising activities, its Notice of Privacy Practices must include a separate statement that the dental practice may contact individuals to raise funds for the dental practice, and that individuals have a right to opt out of receiving such communications.

Opt-out in each fundraising communication. Each fundraising communication must provide a clear and conspicuous opportunity to opt out of future fundraising communications. The opt-out method(s) may not impose an undue burden or more than a nominal cost on people who wish to opt out. Opting out should be quick, simple, and inexpensive. A toll-free number, an email address, or a pre-printed, pre-paid postcard for opting out would be appropriate methods. Requiring patients to write and send a letter via U.S. mail would be too burdensome; however, requiring that patients opt out of further fundraising communications

by mailing a pre-printed, pre-paid postcard would not be an undue burden. A dental practice may permit people to opt out of a single fundraising campaign, or to opt out of all future fundraising communications, as long as the communication is clear. Opt-outs must not be limited in time; someone who has opted out must be kept in opt-out status until he or she opts back in.

Limited patient information may be used for fundraising communications. A dental practice may use patient information, or disclose patient information to a business associate or an institutionally related foundation, for fundraising communications, provided the dental practice:

- Limits the patient information to:
    - demographic information relating to a patient, including name, address, other contact information, age, gender, and date of birth
    - dates of health care provided to a patient
    - department of service information
    - treating dentist
    - outcome information (for screening purposes only),[14] and
    - health insurance status
- includes a statement in its Notice of Privacy Practices that the dental practice may contact individuals to raise funds for the dental practice and that individuals have a right to opt out of receiving such communications
- includes with each such fundraising communication a clear and conspicuous opportunity to opt out of receiving any further fundraising communications
- provides a method for opting out that does not cause the individual to incur an undue burden or more than nominal cost
- does not condition treatment or payment on whether someone opts out, and
- does not make fundraising communications to anyone who has opted out.

Minimum necessary. The "minimum necessary" requirement applies to disclosures of patient information for fundraising purposes (Chapter 2, Step 5).

Opting back in. A dental practice may provide a method for people who have opted out of receiving fundraising communications to opt back in. For example, a routine newsletter may provide a telephone number that people can call to be put on a fundraising list.

Data management. To avoid sending a fundraising communication to someone who has opted out, which would be a HIPAA violation, a dental practice undertaking a fundraising campaign should have appropriate data management systems and processes in place to track and flag in a timely manner all people who have opted out.

[14] Outcome information about the patient may be used for screening only; for example, to prevent communications from being sent to patients who experienced a sub-optimal outcome. This information may only be disclosed to a business associate or foundation if the business associate or foundation will provide the screening function.

L. Immunization Records

Applies to: Any covered entity dental practice that wishes to use a simplified process when the dental practice receives a request from a patient, or a patient's parent or guardian, to send proof of immunization to a school.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 9.

Compliance Date: September 23, 2013.

Background: In general, HIPAA requires a dental practice to get a signed written authorization form before disclosing patient information for purposes that are not permitted or required by HIPAA (Chapter 2, Steps 7 and 8).

Prior rule: A dental practice needed a signed authorization form before it could send immunization records to a school.

New requirement: The new rule permits a dental practice send proof of immunization to a school without a signed authorization form in states that have school entry or similar laws, as long as the patient (or parent or guardian) agrees. If the agreement is oral (e.g., over the telephone), the dental practice must document the agreement (for example, by making a notation in the dental record). If the agreement is in writing (for example, by letter or email), the letter or email is sufficient documentation. A signature is not required. A dental practice can still require a signed authorization form if it wishes.

This new rule only applies to immunization records. A dental practice must still require a signed authorization form before sending or telling any other patient information to a school.

When an authorization form is not required. A dental practice may send proof of a patient's immunization to a school if the:

- patient is a student or prospective student of the school
- information is limited to proof of immunization
- school is required by law to have proof of immunization prior to admitting the patient
- the dental practice obtains the agreement, which may be oral, from the:
    - parent or guardian, if the patient is an unemancipated minor,[15] or
    - patient, if the patient is an adult or emancipated minor, and
- the dental practice documents the agreement (a signature is not required).

Documentation.

- When request is in writing, a copy of the request is the documentation.
- When request is oral, the dental practice must document it. Noting the request in the dental record or elsewhere is sufficient documentation.
- A signature is not required on the documentation.

[15] State law determines when a minor is "emancipated." In some states, a minor who is married or who joins the military is considered emancipated. A court may also be able to give permission for emancipation.

State law. Check state laws before changing the dental practice's procedures for sending immunization information to schools, because dental practices must follow state law if it is more stringent than HIPAA. Also, HIPAA permits dental practices to disclose information if "required by law," so if a state law requires a dental practice to disclose immunization information, HIPAA permits the disclosure to the extent that it is required by law.

Request by school. A request by a school is generally ***not*** sufficient to permit the disclosure of patient information under HIPAA.

Definition of school. HIPAA does not define "school." Before sending immunization information without a signed authorization form, a dental practice should confirm that, under applicable law, the intended recipient qualifies as a "school" and that proof of immunization is required by law before the school may admit the patient.

Training. Dental practices who wish to use these less formal procedures instead of requiring a signed authorization form will need to explain the new procedures to staff.

M. Genetic Information

Applies to: All covered entity dental practices.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 3

Compliance Date: September 23, 2013.

Background: HIPAA applies to "protected health information," which this publication simply refers to as "patient information." Generally, protected health information includes the information in a dental practice that identifies or could be used to identify a patient (see Chapter 3). Examples include paper and electronic dental records, billing records, photographs, radiographs, schedules, contact information, spoken information such as conversations about patients, etc.

Prior rule: Under the prior rule, genetic information was considered "protected health information" if it was maintained by the dental practice or a business associate and it identified the patient.

New requirement: The new rule expressly provides that "genetic information" is protected health information covered by HIPAA. The 2013 Final Rule defines genetic information to include:

- information about a patient's genetic test
- information about the genetic test of a patient's family member[16] (including a fetus carried by the patient or a family member, or an embryo legally held by a patient or family member utilizing an assisted reproductive technology)
- the manifestation of a disease or disorder in a patient's family member
- any request for, or receipt of, genetic services by a patient or a patient's family member ("genetic services" means a genetic test, genetic counseling, or genetic education), or
- any request for, or receipt of, participation in clinical research that includes genetic services by a patient or a patient's family member.

ACTION STEPS:

- ☐ Train staff to apply privacy safeguards to all genetic information, whether the information is about a patient, a patient's family member (including distant family members and family members who are not blood relatives), or persons who are or could become dependents under the patient's health plan.

[16] The 2013 Final Rule defines "family member" to include anyone who is or may become eligible for coverage under a group health plan because of that person's relationship to the patient, as well as the patient's relatives up to the fourth degree (see below), whether they are related by blood, marriage, or adoption, and whether or not they are full or half-relatives (e.g., half siblings are treated the same as siblings who share both parents).
(i) First-degree relatives include parents, spouses, siblings, and children.
(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

N. Research

Applies to: All covered entity dental practices that use or disclose patient information for research purposes.

ADA Practical Guide to HIPAA Compliance Privacy and Security Manual Section: Chapter 2, Step 8

Compliance Date: September 23, 2013.

Background: HIPAA contains special provisions about using and disclosing patient information for research purposes. For example, a dental practice generally may not disclose patient information for research without having the patient sign an appropriate authorization form. HIPAA does not govern de-identified information, so authorization is not required before a dental practice discloses properly de-identified patient information for research purposes (Chapter 2, Step 21 and Chapter 3).

While the application of the HIPAA rules to research is beyond the scope of this book, dental practice should be aware that HIPAA applies to uses and disclosures for research purposes, and that the 2013 Final Rule makes certain changes, such as changing requirements for authorization forms and addressing future use of information permissibly obtained. Dental practices that wish to participate in research that requires the use and/or disclosure of identified or partially identified patient information should consult a qualified attorney in their jurisdiction to determine how the HIPAA rules apply to the proposed research project.

3. Government Resources

The HIPAA Rules. The HIPAA Rules are available in the Electronic Code of Federal Regulations:

1. Visit *www.ecfr.gov*.
2. Select "Title 45 — Public Welfare" in the drop-down menu and click on the "Go" button.
3. On the screen that appears, click on "1-199" under "Browser Parts."
4. On the screen that appears, scroll down to "Subchapter C — Administrative Data Standards and Related Requirements."
5. Click on "160" for the ***General Administrative Requirements***, which contains information about HIPAA enforcement and penalties.
6. For the HIPAA Security, Privacy, and Breach Notification Rules click on "164. The General Provisions (Subpart A) at the top of the page that appears applies to all three rules.
    a. For the ***Security Rule,*** click on "Subpart C — Security Standards for Protection of Electronic Protected Health Information."
    b. For the ***Breach Notification Rule,*** click on "Subpart D — Notification in the Case of Breach of Unsecured Protected Health Information."
    c. For the ***Privacy Rule,*** click on "Subpart E — Privacy of Individually Identifiable Health Information."

The 2013 Final Rule. The 2013 Final Rule is available at *https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf*. This 563-page document contains the actual changes to the HIPAA Rules, preceded by a lengthy preamble that discusses the changes and the reasons behind them, and answers certain questions about implementation.

Understanding Health Information Privacy. The Office for Civil Rights provides information about HIPAA compliance at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html*.

Office for Civil Rights HIPAA Frequently Asked Questions. The website of the Office for Civil Rights has an FAQ section that is searchable by keyword or category. The FAQ page is at *http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html*.

Covered Entity Charts. The Centers for Medicare and Medicaid Services has pr epared charts to help persons and entities determine whether they are required to comply with HIPAA. The charts are available at *http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf*.

Office for Civil Rights Sample Business Associate Agreement Provisions. The federal Office for Civil Rights, which is responsible for HIPAA enforcement, has published information about the new requirements for business associate agreements and sample provisions at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html*.

Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care. The Office for Civil Rights has published a health care provider's guide on this topic at This guide may help answer questions about certain aspects of communicating patient information to family, friends, and others. At our publication date, the guide had not been updated to include information about communicating with a deceased patient's family members and others who were involved in the patient's care or payment for care.

Appendix 1.1

Definitions of Key Terms (plain language)

The following simplified definitions are based on the laws and regulations indicated in the number at the end of each definition. Information that is unlikely to apply to dental practices has been omitted from some of the definitions. Refer to Appendix 1.2 (or to the statutes and regulations themselves) for the official definitions. HIPAA definitions change from time to time as new statutes and regulations are adopted. The following definitions are based on laws and regulations that were current as of March 26, 2013.

Access. In general, "access" means the ability to obtain, use or disclose patient information. When used in connection with HIPAA Security, "access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. **45 CFR § 164.304**

Under the HIPAA Privacy Rule, a patient's right of "access" means the patient's right to see and get copies of his or her patient records. **45 CFR § 164.524**

Addressable. When an implementation specification under the HIPAA Security Rule is "addressable," a dental practice must do the following:

1. The dental practice must assess whether the implementation specification is a reasonable and appropriate safeguard in the dental practice's environment (the dental practice must consider whether the implementation specification is likely to contribute to protecting the dental practice's electronic patient information).
2. If the implementation specification ***is*** reasonable and appropriate, the dental practice must implement the implementation specification.
3. If the implementation specification ***is not*** reasonable and appropriate, the dental practice must:
    a. document why it would not be reasonable and appropriate to implement the implementation specification, and
    b. implement an equivalent alternative measure, if the equivalent alternative measure would be reasonable and appropriate.

Business associates and subcontractors must also comply with the HIPAA Security administrative, physical and technical safeguards, so they, too, must go through this process.

Administrative safeguards. The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Administrative safeguards, such as conducting a written risk assessment and providing workforce training, are administrative actions and policies and procedures that a dental practice uses to manage the selection, development, implementation, and maintenance of security measures to protect electronic patient information and to manage the conduct of the dental practice's workforce in protecting patient information. **45 CFR § 164.304**

ANSI stands for the American National Standards Institute. **45 CFR § 160.103**

Authentication means corroborating that a person is the person whom he or she claims to be (for example, a person trying to log onto a dental practice's electronic dental record system). **45 CFR § 164.304**

Availability means that data or information is accessible and useable upon demand by an authorized person. **45 CFR § 164.304**

Breach has two meanings under HIPAA:

1. *Under the Breach Notification Rule*, a "breach" generally means that someone or something acquired, accessed, used or disclosed unsecured patient information in a way that the Privacy Rule does not permit, which compromised the security or privacy of the patient information. Examples of breaches include the loss or theft of a laptop that contains unsecured electronic patient information, disposing of paper patient records in the regular trash without properly shredding them first, and mailing patient information to the wrong address. There are three exceptions to the definition of breach.

   A dental practice must send notification of a breach of unsecured patient information to affected patients, the federal government, and in some cases the media, unless the dental practice can demonstrate that there is a low probability that the information was compromised by conducting a written assessment of the relevant factors, including at least the four required factors.[1] **45 CFR § 164.402**

2. *Breach of the business associate agreement* means violation of a provision in the agreement. For example, a business associate has breached the agreement if the business associate is aware of a "security incident" but does not notify the dental practice. If a business associate breaches the business associate agreement the dental practice may take legal action for breach of contract and HHS can impose civil money penalties directly on the business associate.

Business associate generally means an entity, or a person who is not a member of the dental practice's workforce, that performs a service for the dental practice involving patient information. Examples of business associates include a billing service, collection agency, accounting or law firm; consultant, health information organization, e-prescribing gateway, data transmission company that requires access to patient information on a routine basis; and a company that offers patients personal health records on behalf of the dental practice. A dental practice must have a business associate agreement in place with each of the dental practice's business associates. A business associate's subcontractor that has access to patient information is treated as a downstream business associate (see definition of "subcontractor"). A business associate must have a business associate agreement in place with each of the business associate's subcontractors.

A health care provider, such as a dental laboratory, does not become a business associate when a dental practice discloses patient information to the health care provider for treatment purposes. However, a health care provider may be a business associate of a dental practice if the health care provider performs a service for the dental practice rather than providing treatment for a patient. For example, a dental practice would need a business associate agreement with a health care provider that accesses the dental practice's patient information for purposes of providing training to the dental practice's workforce. **45 CFR § 160.103**

[1] (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.

Civil money penalty or penalty means the penalty amount (in dollars) that the federal government may impose for a HIPAA violation. **45 CFR § 160.103**

CMS stands for Centers for Medicare & Medicaid Services, an agency within the U.S. Department of Health and Human Services. **45 CFR § 160.103**

Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes. **45 CFR § 162.103**

Code set maintaining organization means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part. **45 CFR § 162.103**

Common control exists if an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity. **45 CFR § 164.103**

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. **45 CFR § 164.103**

Compliance date means the date by which a dental practice or business associate must comply with a HIPAA provision or a change to a HIPAA provision. **45 CFR § 160.103**

Confidentiality means the information is not made available or disclosed to unauthorized persons or processes. **45 CFR § 164.304**

Contrary. HIPAA does not preempt "contrary" state law that relates to the privacy of patient information if the state law is more stringent than HIPAA. This means that a dental practice must comply with both HIPAA and any state law (for example, a state medical privacy law or a state data security law) that is contrary to HIPAA and more stringent than HIPAA. "Contrary" means that a dental practice would find it impossible to comply with both the state and the federal requirement, or that the state law would be an obstacle to accomplishing the purpose of the federal law. "More stringent" means that the state law gives more protection to patient information, or gives individuals more rights over patient information. **45 CFR § 160.202**

Correctional institution means a jail, reformatory, detention center, work farm, halfway house, residential community program center, or other penal or correctional facility operated for the confinement or rehabilitation of persons charged with or convicted of a crime, or "other persons held in lawful custody." A correctional institution may be operated by or under contract to the U.S., a state, territory, political subdivision of a state or territory, or an Indian tribe. "Other persons held in lawful custody" includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. **45 CFR § 164.501**

Covered Entity means:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider (such as a dental practice) that transmits any health information in electronic form in connection with a transaction covered by HIPAA. **45 CFR § 160.103**

Covered functions means those functions of a dental practice that make the practice a health care provider. **45 CFR § 164.103**

Data aggregation means that a business associate will combine a dental practice's patient information with patient information of other covered entities (such as other dental practices) to permit data analyses that relate to the health care operations of the respective covered entities. **45 CFR § 164.501**

Data element means the smallest named unit of information in a transaction. **45 CFR § 162.103**

Data set means a semantically meaningful unit of information exchanged between two parties to a transaction. **45 CFR § 162.103**

De-identified. In general, patient information is "de-identified" if 18 identifiers (name, address, etc.) are removed, and the remaining information cannot be used alone or in combination with other information to identify the patient. HIPAA does not apply to properly de-identified information.

Descriptor means the text defining a code. **45 CFR § 162.103**

Designated record set means a group of records maintained by or for a dental practice that is:

a. the medical records and billing records about patients maintained by or for the dental practice, or

b. used, in whole or in part, by or for the dental practice to make decisions about patients.

For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for the dental practice. **45 CFR § 164.501**

Direct treatment relationship means a treatment relationship between a patient and a health care provider that is not an indirect treatment relationship. **45 CFR § 164.501**

Direct data entry means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer. **45 CFR § 162.103**

Disclosure means releasing, transferring, providing access to, or divulging information in any manner outside the dental practice or other entity holding the information. **45 CFR § 160.103**

Electronic health record (EHR) means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. **HITECH Act, § 13400**

Electronic media means:

1. Electronic storage media on which data is or may be recorded electronically, such as computer hard drives and removable/transportable memory medium, such as USB drives, CD-ROMs, digital memory cards, magnetic tape or disks, and optical disks.

2. Transmission media used to exchange information already in electronic storage media, such as the Internet, extranet, or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Certain transmissions, including of paper, via fax, and of voice, via telephone, are not considered to be "transmissions via electronic media" if the information being exchanged did not exist in electronic form before the transmission. **45 CFR § 160.103**

Electronic protected health information means protected health information (patient information) that is transmitted by electronic media or maintained in electronic media. Examples include patient information on a desktop or laptop, in an electronic dental record, in an electronic practice management system, in an email, in an electronic document (such as Word or .pdf), or on removable media such as a CD-ROM or a USB drive. **45 CFR § 160.103**

Employer is defined as it is in the federal law governing withholding taxes, 26 U.S.C. 3401(d). **45 CFR § 160.103**

Encryption means 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. **45 CFR § 164.304**

Facility means the physical premises and the interior and exterior of a building(s). **45 CFR § 164.304**

Family member means a person's dependent, which means someone who is or may become eligible for coverage under the terms of a group health plan because of a relationship to a participant, or one of the following relatives by marriage, adoption, or blood (blood relatives include partial blood relatives, such as half-siblings):

- Parents, spouses, siblings, and children.
- Grandparents, grandchildren, aunts, uncles, nephews, and nieces.
- Great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
- Great-great grandparents, great-great grandchildren, and children of first cousins. **45 CFR § 160.103**

Format refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction. **45 CFR § 162.103**

Genetic information means information about the following that pertains to (1) a patient, (2) a family member of a patient (see definition of "family member"), (3) a fetus carried by the patient or a family member of a patient, or (4) an embryo legally held by a patient or a patient's family member using an assisted reproductive technology:

- A genetic test (see definition of "genetic test").
- Request for genetic services (see definition of "genetic services").
- Receipt of genetic services (see definition of "genetic services").
- Participation in clinical research which includes genetic services.

Genetic information also includes the manifestation of a disease or disorder in family members of a patient (see definition of "manifested").

Genetic information does not include information about the sex or age of any patient. **45 CFR § 160.103**

Genetic services means:

1. A genetic test.
2. Genetic counseling (including obtaining, interpreting, or assessing genetic information).
3. Genetic education. **45 CFR § 160.103**

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. **45 CFR § 160.103**

HHS stands for the U.S. Department of Health and Human Services. **45 CFR § 160.103**

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. **45 CFR § 160.103**

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. **45 CFR § 160.103**

Health care operations. The definition of health care operations is important because HIPAA generally permits a dental practice to use and disclose patient information for health care operations purposes without having the patient sign a written authorization form. However, there are exceptions, such as subsidized marketing communications and sale of patient information.

"Health care operations" is a broad category of dental practice activities such as business management and general administrative activities of the dental practice (for example, HIPAA compliance, customer service, resolving internal grievances, the sale of the practice to another covered entity (or to an entity that will become a covered entity following the sale) and due diligence related to the sale, and de-identifying PHI). Other examples include business planning and development (such as cost-management and planning related analyses), conducting quality assessment and improvement activities, certain patient safety activities, case management and care coordination, reviewing the competence or qualifications of health care professionals, conducting training programs in which health care students, trainees, or practitioners learn under supervision, training of non-health care professionals, licensing and credentialing activities, arranging for legal services, and auditing (including fraud and abuse detection and compliance programs). To determine whether an activity is a health care operation, consult the full definition in **45 CFR 160.103**.

Health care provider means a person or organization that furnishes, bills, or is paid for health care in the normal course of business. Dental practices and dental laboratories providing treatment to patients are examples of health care providers. **45 CFR § 160.103**

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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. **45 CFR § 160.103**

Health information technology means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designated for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. **HITECH Act, § 3000**

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. **45 CFR § 164.501**

Health plan generally means an individual or group plan or combination of plans that provides or pays for the cost of medical care. Examples of health plans include employee welfare benefit plans, HMOs, Medicare, the Medicare Advantage program, an issuer of a Medicare supplemental policy, Medicaid, an approved State child health plan, the veterans health care program, CHAMPUS, the Indian Health Service, and the Federal Employees Health Benefits Program. Health plan also includes the Medicare Voluntary Prescription Drug Program (Medicare Part D), and issuers of certain long-term care policies.

Health plan generally excludes accident/disability income insurance, liability insurance (including auto) and supplements to liability insurance, worker's comp, auto medical payment insurance, credit-only insurance, coverage for on-site medical clinics, and government-funded programs (except the ones listed above) whose principal purpose is not providing, or paying the cost of, health care, or whose principal activity is directly providing health care to persons or making grants to fund the direct provision of health care to persons. **45 CFR § 160.103**

Implementation specification means specific requirements or instructions for implementing a standard. **45 CFR § 160.103**

Indirect treatment relationship. An example of an "indirect treatment relationship" is where (1) a health care provider provides health care to patients based on orders of a dental practice, and (2) typically, the health care provider provides services or products, or reports the diagnosis or results, directly to the dental practice, and the dental practice provides the services, products, or reports to the patients. **45 CFR § 164.501**

Individual means the person who is the subject of protected health information. For a dental practice, the individual usually means the patient. **45 CFR § 160.103**

Individually identifiable health information is health information, including demographic information such as names, addresses, genders, etc., and genetic information, that (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 a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient, and (3) that identifies the patient or could be used to identify the patient. **45 CFR § 160.103**

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. **45 CFR § 164.304**

Integrity means that data or information have not been changed or destroyed in an unauthorized manner. **45 CFR § 164.304**

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. **45 CFR § 164.103 & 164.501**

Maintain or maintenance, when used in the HIPAA Security Rule, refers to activities necessary to support the use of a standard adopted by HHS, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification. **45 CFR § 162.103**

Malicious software means software, for example, a virus, designed to damage or disrupt a system. **45 CFR § 164.304**

Manifestation or manifested means that a person has been, or could reasonably be, diagnosed with a disease or disorder by a health care professional with appropriate training and expertise in appropriate the field of medicine. For HIPAA purposes, a disease, disorder, or pathological condition is not "manifested" if the diagnosis is based principally on genetic information. **45 CFR § 160.103**

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. However, marketing does not include: (1) certain communications made for treatment, case management, or care coordination purposes *unless* the dental practice receives "financial remuneration" (dollars) in exchange for making the communication, and (2) certain refill reminders. With certain exceptions, if a dental practice will receive financial remuneration for making a marketing communication, the dental practice must have patients sign HIPAA-compliant authorization forms that state that the dental practice will receive financial remuneration for making the communication. **45 CFR § 164.501**

Maximum defined data set means all of the required data elements for a particular standard based on a specific implementation specification. **45 CFR § 162.103**

More stringent. A state law is more stringent than HIPAA if the state law:

1. prohibits or restricts a use or disclosure that would be permitted under HIPAA (unless the disclosure is to the patient about his or her own information, or to HHS for determining HIPAA compliance).
2. gives patients greater rights than HIPAA to see or get copies of their records, or ask the dental practice to change information in their records.
3. gives patients greater rights to information about a use, disclosure, rights, and remedies than HIPAA.
4. with respect to authorization forms and other legal permissions from patients, has narrower scope or duration, more privacy protections, or less coercive effect of the circumstances surrounding the permission than HIPAA.

5. requires dental practices to retain or report more detailed information, or to retain or report information for a longer period of time, than HIPAA's recordkeeping or accounting of disclosures requirements.

6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the patient information. **45 CFR § 160.202**

National Coordinator means the head of the Office of the National Coordinator for Health Information Technology established under section 3001(a). **HITECH Act, § 3000**

Payment generally means the dental practice's activities to obtain reimbursement or compensation for service performed or products provided and a health plan's activities to collect premiums, determine the plan's responsibility to provide coverage and benefits, and provide coverage and benefits. Examples of "payment" activities include things like determinations of eligibility or coverage, coordination of benefits, determination of cost sharing amounts, billing, claims management, collection activities, review of medical necessity, coverage, appropriateness of care or justification of charges, utilization review, including precertification and preauthorization, concurrent and retrospective review of services, and disclosure of limited information to consumer reporting agencies relating to collection of premiums or reimbursement (names and addresses, date of birth, Social Security number, payment history, account number, and name/address of health care provider and/or health plan). **45 CFR § 164.501**

Physical safeguards. The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Physical safeguards, such as door locks, workstation use and security, and disposal of electronic hardware and software, are physical measures, policies, and procedures to protect a dental practice's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. **45 CFR § 164.304**

Privacy Official means the person the dental practice designates to develop and implement the dental practice's policies and procedures to comply with the Privacy Rule.
45 CFR § 164.530(a)(1)(i)

Privacy Rule means the HIPAA Privacy Rule. **45 CFR § 164.500 through 45 CFR § 164.532**

Protected health information ("PHI") generally means patient information, including demographic information (names, addresses, genders, etc.), genetic information (see definition of "genetic information"), dental records, billing records, and any other information in the dental practice about a patient's health, treatment, or payment for health care. PHI includes information in any form or format, such as electronic, hard copy (paper records, photos, films, etc.) and spoken information. PHI does not include properly de-identified information (Chapter 2, Step 21), or information about a patient who has been deceased for 50 years or more (Chapter 1.H.1) The definition of PHI also excludes certain education records, and employment records held by a dental practice in its role as employer. **45 CFR § 160.103**

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. **45 CFR § 164.501**

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from, or contract with, such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. **45 CFR § 164.501**

Reasonable cause means an act or omission in which a dental practice or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated a HIPAA provision, but in which the dental practice or business associate did not act with willful neglect. **45 CFR § 160.401**

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. **45 CFR § 164.401**

Required. When a HIPAA Security Rule standard includes a "required" implementation specification, a dental practice must implement the implementation specification. Business associates and subcontractors must also comply with the HIPAA Security administrative, physical and technical safeguards, so they, too, must go through this process. **45 CFR § 164.306(d)**

Required by law means a mandate contained in law that requires a dental practice to use or disclose patient information and that is enforceable in a court of law. Examples of uses and disclosures required by law includes court orders and court-ordered warrants, subpoenas and summons, Medicare conditions of participation, and statutes or regulations that require patient information if a dental practice seeks payment under a government program providing public benefits. **45 CFR § 164.103**

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. **45 CFR § 164.501**

Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or any other officer or employee of HHS to whom the authority involved has been delegated. **45 CFR § 160.103**

Secured. If patient information is properly "secured," a dental practice does not need to send breach notification if the information is lost or stolen, or used, disclosed, accessed or acquired in violation of the Privacy Rule. Electronic patient information can be secured through appropriate encryption. Hard copy patient information cannot be secured except though appropriate destruction. Encryption and destruction requirements are in the Breach Notification Rule *Guidance*. **45 CFR § 164.402**

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system. **45 CFR § 164.304**

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. **45 CFR § 164.304**

Security Official means the person a dental practice designates to develop and implement the policies and procedures required by the Security Rule. Business associates and subcontractors must also designate Security Officials. **45 CFR § 164.308(a)(2)**

Standard means a rule, condition, or requirement under the HIPAA Security or Privacy Rule. **45 CFR § 160.103**

Standard transaction means a transaction that complies with an applicable standard adopted under the Administrative Requirements of the HIPAA regulations. **45 CFR § 162.103**

State. Under HIPAA, "state" generally means any of the U.S. states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam, American Samoa and the Commonwealth of the Northern Mariana Islands. For a health plan established or regulated by Federal law, "state" has the meaning set forth in the applicable section of the United States Code for such health plan. **45 CFR § 160.103**

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. **45 CFR § 160.202**

Subcontractor. A person or entity is a "subcontractor" of a business associate if a business associate delegates a function, activity, or service to the person or entity; however, the business associate's workforce members are not subcontractors. **45 CFR § 160.103**

Technical safeguards. The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Technical safeguards, such as unique usernames, automatic logoff, and encryption, means the technology, and the policy and procedures for its use, that protect electronic patient information and control access to it. **45 CFR § 164.304**

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Other transactions that the Secretary may prescribe by regulation. **45 CFR § 160.103**

Treatment means providing, coordinating, or managing health care and related services by one or more health care providers, including coordinating or managing health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. **45 CFR § 164.501**

Unsecured. See "Secured."

Use means, with respect to patient information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. **45 CFR § 160.103**

User means a person or entity with authorized access. **45 CFR § 164.304**

Violation or violate means, as the context may require, failure to comply with a HIPAA provision. **45 CFR § 160.103**

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA provision that was violated. **45 CFR § 160.401**

Workforce. A dental practice's workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a dental practice, is under the direct control of the dental practice, whether or not they are paid by the dental practice. A business associate's workforce means the business associate's employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the business associate, is under the direct control of the business associate, whether or not they are paid by the business associate. **45 CFR § 160.103**

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. **45 CFR § 164.304**

Appendix 1.2
Definitions of Key Terms (regulatory language)

The following HIPAA definitions of key terms are current as of March 26, 2013. The definitions are from the Code of Federal Regulations ("CFR") Title 45, Subtitle A, Subchapter C, Parts 160, 162 and 164. A copy of these regulations can be found online in the *Electronic Code of Federal Regulations* at *http://ecfr.gpoaccess.gov*.

At the end of each definition, in bold, is a number that indicates the statute or regulation where the definition is located. For example, the definition of "administrative safeguards" can be found in **45 CFR § 164.304.**

For simplified versions of definitions, see Appendix 1.1, "Definitions of Key Terms." The definitions in Appendix 1.1 have been simplified and paraphrased, and in some cases information is omitted that is unlikely to apply to most dental practices.

HIPAA definitions change from time to time as new statutes and regulations are adopted.

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.) **45 CFR § 164.304**

Act means the Social Security Act. **45 CFR § 160.103**

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. **45 CFR § 164.304**

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;

(2) Section 264 of Pub. L. 104-191;

(3) Sections 13400-13424 of Public Law 111-5; or

(4) This subchapter. **45 CFR § 160.103**

ALJ means Administrative Law Judge. **45 CFR § 160.103**

ANSI stands for the American National Standards Institute. **45 CFR § 160.103**

Authentication means the corroboration that a person is the one claimed. **45 CFR § 164.304**

Availability means the property that data or information is accessible and useable upon demand by an authorized person. **45 CFR § 164.304**

Board means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three. **45 CFR § 160.502**

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to
retain such information.

(2.) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.
45 CFR § 164.402

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

4. Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services. **45 CFR § 160.103**

Civil money penalty or penalty means the amount determined under **§ 160.404** of this part and includes the plural of these terms. **45 CFR § 160.103**

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services. **45 CFR § 160.103**

Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes. **45 CFR § 162.103**

Code set maintaining organization means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part. **45 CFR § 162.103**

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. **45 CFR § 164.103**

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. **45 CFR § 164.103**

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter. **45 CFR § 160.103**

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes. **45 CFR § 164.304**

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable. **45 CFR § 160.202**

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. **45 CFR § 164.501**

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. **45 CFR § 160.103**

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. **45 CFR § 164.103**

Covered health care provider means a health care provider that meets the definition at paragraph (3) of the definition of "covered entity" at §160.103 of this subchapter. **45 CFR § 162.103**

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities. **45 CFR § 164.501**

Data condition means the rule that describes the circumstances under which a covered entity must use a particular data element or segment. **45 CFR § 162.103**

Data content means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not data content. **45 CFR § 162.103**

Data element means the smallest named unit of information in a transaction. **45 CFR § 162.103**

Data set means a semantically meaningful unit of information exchanged between two parties to a transaction. **45 CFR § 162.103**

Descriptor means the text defining a code. **45 CFR § 162.103**

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. **45 CFR § 164.501**

Designated standard maintenance organization (DSMO) means an organization designated by the Secretary under §162.910(a). **45 CFR § 162.103**

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. **45 CFR § 164.501**

Direct data entry means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer. **45 CFR § 162.103**

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. **45 CFR § 160.103**

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents. **45 CFR § 160.103**

Electronic health record (EHR) means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. **HITECH Act, § 13400**

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, 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 if the information being exchanged did not exist in electronic form immediately before the transmission. **45 CFR § 160.103**

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section. **45 CFR § 160.103**

Employer is defined as it is in 26 U.S.C. 3401(d). **45 CFR § 160.103**

Encryption means 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. **45 CFR § 164.304**

Facility means the physical premises and the interior and exterior of a building(s). **45 CFR § 164.304**

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in **45 CFR 144.103**), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins. **45 CFR § 160.103**

Format refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction. **45 CFR § 162.103**

Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual. **45 CFR § 160.103**

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education. **45 CFR § 160.103**

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. **45 CFR § 160.103**

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan. **45 CFR § 160.103**

HCPCS stands for the Health [Care Financing Administration] Common Procedure Coding System. **45 CFR § 162.103**

HHS stands for the Department of Health and Human Services. **§ 160.103**

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. **45 CFR § 160.103**

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. **45 CFR § 160.103**

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with §164.105(a)(2)(iii)(C). **45 CFR § 164.103**

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in **42 CFR 3.20**); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. **45 CFR § 164.501**

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. **45 CFR § 160.103**

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, 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. **45 CFR § 160.103**

Health information technology means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designated for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. **HITECH Act, § 3000**

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan. **45 CFR § 160.103**

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO. **45 CFR § 160.103**

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. **45 CFR § 164.501**

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons. **45 CFR § 160.103**

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(C). **45 CFR § 164.103**

Implementation specification means specific requirements or instructions for implementing a standard. **45 CFR § 160.103**

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. **45 CFR § 164.501**

Individual means the person who is the subject of protected health information. **45 CFR § 160.103**

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

(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. **45 CFR § 160.103**

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. **45 CFR § 164.304**

Inmate means a person incarcerated in or otherwise confined to a correctional institution. **45 CFR § 164.501**

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner. **45 CFR § 164.304**

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. **45 CFR § 164.103**

Maintain or maintenance refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification. **45 CFR § 162.103**

Malicious software means software, for example, a virus, designed to damage or disrupt a system. **45 CFR § 164.304**

Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information. **45 CFR § 160.103**

Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual. 45 CFR § 164.501

Maximum defined data set means all of the required data elements for a particular standard based on a specific implementation specification. **45 CFR § 162.103**

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification. **45 CFR § 160.103**

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information. **45 CFR § 160.202**

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans. **45 CFR § 160.103**

Password means confidential authentication information composed of a string of characters. **45 CFR § 164.304**

Payment means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social Security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan. **§ 164.501**

Person means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private. **45 CFR § 160.103**

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. **45 CFR § 164.304**

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B). **45 CFR § 164.103**

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.
45 CFR § 160.103

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy* notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. **45 CFR § 164.501**

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. **45 CFR § 164.501**

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. **45 CFR § 160.401**

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. **45 CFR § 164.401**

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way. **45 CFR § 160.202**

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. **45 CFR § 164.103**

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. **45 CFR § 164.501**

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty. **45 CFR § 160.103**

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated. **45 CFR § 160.103**

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system. **45 CFR § 164.304**

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. **45 CFR § 164.304**

Segment means a group of related data elements in a transaction. **45 CFR § 162.103**

Small health plan means a health plan with annual receipts of $5 million or less. **45 CFR § 160.103**

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information. **45 CFR § 160.103**

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part. **45 CFR § 160.103**

Standard transaction means a transaction that complies with an applicable standard adopted under this part. **45 CFR § 162.103**

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.
45 CFR § 160.103

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. **45 CFR § 160.202**

Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
45 CFR § 160.103

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. **45 CFR § 164.304**

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.) **45 CFR § 160.103**

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health claims attachments.

(11) Other transactions that the Secretary may prescribe by regulation. **45 CFR § 160.103**

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. **45 CFR § 164.501**

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. **45 CFR § 164.402**

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. **45 CFR § 160.103**

User means a person or entity with authorized access. **45 CFR § 164.304**

Violation or violate means, as the context may require, failure to comply with an administrative simplification provision. **45 CFR § 160.103**

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. **45 CFR § 160.401**

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. **45 CFR § 160.103**

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. **45 CFR § 164.304**