PRACTICAL GUIDE SERIES

Chapter 2

25 Steps Toward Privacy and Breach Notification Compliance

What You Will Learn in This Chapter

- Understand 25 steps toward HIPAA privacy compliance
- Use the sample policies and procedures and sample forms as tools to help you tailor and update your dental practice's policies and procedures.
- Identify topics that must be addressed in training of your workforce members (including management).

Key Terms

Below are some key terms used in this chapter. See Appendix 1.1 for plain-language definitions and Appendix 1.2 official definitions of HIPAA 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.

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

Breach
Business Associate
Contrary
Data Aggregation
Designated Record Set
De-identified
Disclosure
Electronic Media
Family Member
Genetic Information
Health Care Operations
Health Plan
Law Enforcement Official
Marketing
More Stringent
Payment
Privacy Official
Secured
Treatment
Use
Workforce

[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 2

25 Steps Toward Privacy and Breach Notification Compliance

This chapter summarizes the parts of the Privacy Rule that are most likely to apply to dental practices and provides sample policies and procedures and forms that pertain to specific aspects of the Privacy Rule.

The "25 Steps" are not arranged in chronological order and a dental practice should complete all of the Steps as quickly as reasonably possible. None of the Steps is a prerequisite to any of the others — never wait to start on a Step merely because you have not completed a prior Step.

For example, if a dental practice discovers a suspected breach of unsecured patient information (Chapter 2, Step 22), it must investigate and send any required notification in a timely manner, even if it has not yet designated a Privacy Official (Chapter 2, Step 1). Similarly, if a dental practice does not have a written business associate agreement in place with a business associate (Chapter 2, Step 13), the dental practice must enter into a compliant written agreement without delay, even if it has not yet completed its policies and procedures (Chapter 2, Step 2).

In addition to complying with the Privacy Rule, a dental practice must also comply with other applicable federal laws, and with state laws that are more stringent than, HIPAA (for example, state laws that give patients more rights than HIPAA, or that provide more protection to patient information than HIPAA does). Consult a qualified attorney in your jurisdiction to make sure your dental practice is in compliance with HIPAA and with any applicable state laws.

How to find the HIPAA Rules. This chapter frequently refers to the HIPAA Rules by number. For example, the Privacy Rule requirement to designate a Privacy Official is in "45 CFR 164.530(a)". The text of the HIPAA Rules are available in the Electronic Code of Federal Regulations. To look up a rule:

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. For the HIPAA Privacy, Security 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 ***Privacy Rule,*** click on "Subpart E — Privacy of Individually Identifiable 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 ***Security Rule,*** click on "Subpart C — Security Standards for Protection of Electronic Protected Health Information."

A summary of the Privacy Rule is available on the website of the federal Office for Civil Rights ("OCR") at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html*. The OCR also offers answers to frequently asked questions about HIPAA on its website, at *http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html*.

DISCLAIMER. Sample policies and procedures presented throughout this HIPAA Privacy and Security Kit are for reference purposes only and are not intended to be, nor shall they be construed as, legal advice. Consult a qualified attorney in your jurisdiction to advise you as you draft and implement HIPAA policies and procedures for your dental practice and as questions arise about your policies, procedures, and compliance. These sample policies and procedures refer to federal, not state law. Consult a qualified attorney in your jurisdiction or your state dental society for more information about the privacy laws of your state.

25 Steps Toward Privacy and Breach Notification Compliance

1. Choose a Privacy Official.
2. Write your privacy policies and procedures and put them into action.
3. Write and provide your Notice of Privacy Practices.
4. Make a list of your Designated Record Sets .
5. Follow the Minimum Necessary Requirement.
   - 5.1 Restrict workforce access to patient information.
   - 5.2 Make rules for routine disclosures and requests for patient information.
   - 5.3 Analyze non-routine disclosures and requests for patient information.
   - 5.4 Respond appropriately to third party requests for patient information.
6. Verify identity before disclosing patient information.
7. Understand when a dental practice is required to disclose patient information.
8. Understand when a dental practice is permitted to use and disclose patient information without having the patient sign an authorization form.
9. Learn when patient authorization forms are required and what they must say.
10. Do not send subsidized marketing communications without patients' written authorization.
11. Do not "sell" patient information without patients' written authorization unless an exception applies.
12. Mitigate (lessen) the harm of any improper use or disclosure.
13. Have business associate agreements in place and manage business associates appropriately.
    - 13.1 Who are your dental practice's business associates?
    - 13.2 What if a business associate violates HIPAA or the business associate agreement?
    - 13.3 When a business associate is an agent?
14. Respond appropriately to patient requests.
    - 14.1 If a patient asks to see or get a copy of his or her patient information.
    - 14.2 If a patient asks to change his or her patient information.
    - 14.3 If a patient asks for an accounting of disclosures of his or her patient information.
    - 14.4 If a patient asks to receive communications by a different means or at a different place.
    - 14.5 If a patient asks the dental practice not to disclose his or her patient information.
15. Train your workforce on privacy and breach notification.
16. Have and apply appropriate sanctions (disciplinary action) for workforce HIPAA violations.
17. Prohibit retaliation and intimidation.
18. Do not require improper waivers of HIPAA rights.
19. Maintain documentation of HIPAA compliance.
20. Safeguard patient information in all formats.
21. Learn how to de-identify patient information.
22. Comply with the Breach Notification Rule.
23. Handle complaints properly.
24. Do not use patient information for fundraising without proper authorization or opt-out.
25. Review your privacy program periodically and revise as necessary.

Step 1: Privacy Official

Choose a Privacy Official and make the other personnel designations required by the Privacy Rule. Make sure to document the designations.

Where to find the rules:

45 CFR 164.530(a)
45 CFR 164.524(e)(2)

What is required:

The Privacy Rule requires a dental practice to designate personnel to fill the following five roles, and to document the designations (see *Sample Designation of Privacy Official*, Appendix 2.1.1):

- A Privacy Official, who is responsible for developing the dental practice's privacy policies and procedures and putting them into action
- A contact person who is responsible for receiving complaints and for providing further information about the Notice of Privacy Practices (Chapter 2, Step 23)
- A person responsible for receiving and processing patient requests to see or get copies of their information. (Chapter 2, Step 14.1)
- A person responsible for receiving and processing requests for accountings of disclosures (Chapter 2, Step 14. 3)
- A person responsible for receiving and processing requests to amend (change) patient records (Chapter 2, Step 14.2)

A dental practice may wish to have the same person fulfill all these roles. In some dental practices, the Privacy Official also serves as the Security Official, who is responsible for writing up security policies and procedures to safeguard electronic patient information and putting them into action (see Chapter 4).

These are important assignments. Make sure that these roles are filled by a person capable of taking on a high level of responsibility. The Privacy Official should be mature, experienced, able to think on his or her feet, and familiar with all aspects of practice operations.

A dental practice must document these designations and update the documentation whenever a new person is designated to take over any of these duties. Retain the documentation for at least six years from the date of its creation or the date when it last was in effect, whichever is later (Chapter 2, Step 19).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice's Privacy Official shall be responsible for developing and implementing our HIPAA privacy and breach notification policies and procedures, receiving complaints about our privacy and breach notification practices, providing further information about our Notice of Privacy Practices, and receiving and processing requests for access, amendment, and accountings of disclosure.

SAMPLE POLICY AND PROCEDURES

Sample Procedures

Staff: Our Privacy Official is responsible for developing privacy and breach notification policies and procedures and putting them into action. Examples of these policies and procedures include how to protect patient privacy, how you are permitted to use, disclose and request information about patients, and how to respond to requests from patients and others concerning dental records and other information.

Privacy Official: You are responsible for developing and implementing privacy and breach notification policies and procedures and updating them as appropriate. The policies and procedures will apply to patient information in oral, written and electronic form. Your duties include, but are not limited to, the responsibilities listed in the Privacy Official job description.

Sample Forms:

- *Sample Designation of Privacy Official,* Appendix 2.1.1
- *Sample Privacy Official Job Description*, Appendix 2.1.2

Appendix 2.1.1

Sample Designation of Privacy Official

This sample form illustrates how a dental practice might document its designation of the Privacy Official and make other documented personnel designations that the Privacy Rule requires.

_____

{NAME OF PRACTICE}

Effective _____ (date),

_____ (Name of Dental Practice)

designates _____ (name)

as:

- The Privacy Official, responsible for developing and implementing the dental practice's privacy policies and procedures, and as
- The person responsible for:
  - o receiving complaints
  - o providing further information about the Notice of Privacy Practices (for example, to patients, staff, etc.), and
  - o receiving and processing:
    - requests for access
    - accountings of disclosures
    - requests for amendment

Appendix 2.1.2
Sample Privacy Official Job Description

This sample form illustrates how a dental practice might write a job description for the Privacy Official.

General Duties:

Maintain the privacy of patient information and oversee activities that keep our practice in compliance with the HIPAA Privacy and Breach Notification Rule and applicable state laws on privacy, data security, and patient records.

Specific Duties:

The Privacy Official has the following specific duties:

- **Management Advisor**
  Work with the dental practice's management team and lawyers to comply with applicable federal and state laws. Stay current on privacy laws and updates in privacy technology. Immediately notify the Dentist[1] of any communication from or on behalf of a governing agency, such as the Office for Civil Rights or the state attorney general, (for example, if the dental practice receives a communication about a notice of investigation, compliance review, or audit).

- **Policies and Procedures**
  Develop, or serve as team leader in the development of, compliant privacy and breach notification policies and procedures. Implement the policies and procedures and integrate them into the practice's day-to-day activities.

- **Training and Sanctions**
  Provide timely training (planned courses, updates, reminders, and on-the-spot refreshers) to all workforce members, including management, employees, temps, trainees, volunteers, and others whose work for our dental practice is under the practice's direct control. Oversee sanctions for violations of HIPAA and our privacy policies and procedures according to our human resources policies, and bring any sanctions to the attention of the Dentist.

- **Risk Management**
  Collaborate with the Security Official to ensure that privacy and security risks are analyzed, documented and updated as appropriate.

- **Business Associates**
  Ensure that appropriate agreements are in place with each of our dental practice's business associates. Lead the practice in developing and updating business associate agreements and work with the management team and lawyers to develop and execute compliant business associate agreements.

- **Patient Rights**
  Respond to patient requests regarding their information and to questions about our privacy practices. Maintain documentation related to patient requests. Help the practice's employees understand how to respond appropriately to patient questions about their information and our privacy practices.

[1] In some larger practices or dental groups the person to be notified immediately is the Practice Administrator or Executive Director.

- **Documentation**
  Create, receive, and maintain documentation related to our privacy practices, and retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. Organize documentation for prompt retrieval in the event of a government investigation or audit.

- **Complaint Management**
  Receive, respond to, and document complaints about our privacy practices, investigating complaints and mitigating harm where appropriate. Educate workforce on our policies and procedures on complaints, and that retaliation and intimidation is prohibited against individuals who exercise their patient rights.

- **Qualifications**
  Must be familiar with dental and administrative functions of the practice; have excellent communication, problem solving, and research skills and an interest in privacy laws and regulations; be recognized as detail-oriented and having high integrity; have strong organizational skills and work well with management and staff.

Step 2: Privacy Policies and Procedures

Write up your privacy and breach notification policies and procedures and put them into action. Update your policies and procedures to reflect changes in the law and changes in your privacy practices.

Where to find the rules:

45 CFR 164.530(i)

What is required:

Dental practices must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule and the Breach Notification Rule. Your policies and procedures should also comply with applicable state laws. HIPAA does not pre-empt state law that is contrary to HIPAA if the state law is more stringent than the HIPAA requirement.

The HIPAA Privacy and Breach Notification Rules apply to patient information in any format, such as electronic, hard copy (for example, paper records, photographs, films and radiographs) and oral (spoken) information.

The policies and procedures must be reasonably designed, taking into account the size of the dental practice and the type of the dental practice's activities that relate to patient information. The policies and procedures must ensure compliance with HIPAA, and may not permit a violation of a HIPAA requirement.

A dental practice must change its policies and procedures as necessary and appropriate to comply with changes in HIPAA Privacy and Breach Notification Rules, and with changes in the dental practice's privacy practices. Whenever there is a change in the law that necessitates a change to policies and procedures, the dental practice must promptly document and implement the revised policies or procedures.

If the change in law materially affects the content of the dental practice's Notice of Privacy Practices, the dental practice must promptly make the appropriate revisions to the Notice (Chapter 2, Step 3). Make sure that the revised policies and procedures comply with HIPAA. Document the change in the policies and procedures, revise the Notice, and do not implement the change before documenting it in the policies and procedures or before the effective date of the revised Notice.

ADA TIP

Although not a HIPAA requirement, a dental practice may be prudent to ask workforce members to sign an acknowledgment form that they received a copy of the dental practice's privacy and breach notification policies and procedures, understand them, and will comply (see *Sample Acknowledgement of Receipt of HIPAA Policies and Procedures,* Appendix 2.2).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will develop and implement policies and procedures to comply with the HIPAA Privacy and Breach Notification Rule, as well as applicable state laws. We will revise our policies and procedures promptly as appropriate when there is change in the law or in our privacy practices.

Sample Procedures

Staff: Our dental practice has privacy and breach notification policies and procedures. The policies and procedures will be updated from time to time. All workforce members must comply with the policies and procedures when they do their jobs.

Privacy Official: You are responsible for developing, implementing and documenting our privacy and breach notification policies and procedures, and for updating them as necessary — for example, if our privacy practices change, if the HIPAA rules change, or if there is a change in state law.

Provide all members of our workforce with a paper or electronic copy of the privacy, security and breach notification policies and procedures, and any revisions, and keep a current copy readily accessible to all workforce members.

When there is a change in the law or in our privacy practices, revise the policies and procedures (and if necessary, the Notice of Privacy Practices) as appropriate prior to the effective date of the change.

Sample Form:

- *Sample Acknowledgment of Receipt of HIPAA Policies and Procedures,* Appendix 2.2

Appendix 2.2

Sample Acknowledgement of Receipt of HIPAA Policies and Procedures

This sample form illustrates how a dental practice might obtain acknowledgement of receipt from each workforce member that he or she has received a copy (in paper or electronic format) of the practice's privacy, security and breach notification policies and procedures.

_____

{NAME OF PRACTICE}

I have received and reviewed a copy of our dental practice's privacy, security and breach notification policies and procedures.

I understand that I should ask our dental practice's Privacy Official if I have any questions about these policies and procedures.

Print Name: _____

Signature: _____

Date: _____

Apéndice 2.2b

Ejemplo de acuse de recibo de las políticas y los procedimientos de la HIPAA

Este formulario de ejemplo ilustra cómo un consultorio odontológico podría obtener acuse de recibo, por parte de cada miembro del personal, que indique que él o ella ha recibido una copia (en papel o en formato electrónico) de las políticas y los procedimientos de privacidad, seguridad y notificación de infracciones.

_____

{Nombre del consultorio}

He recibido de nuestro consultorio odontológico una copia de las políticas y los procedimientos de seguridad, privacidad y notificación de infracciones, y los he revisado.

Entiendo que, si tengo alguna duda respecto de estas políticas y estos procedimientos, debo consultar con el funcionario de privacidad de nuestro consultorio odontológico.

Nombre en letra de molde: _____

Firma: _____

Fecha: _____

Step 3: Notice of Privacy Practices ("Notice" or "NPP")

Write and provide your Notice of Privacy Practices, and revise it when appropriate.

Where to find the rules:

45 CFR 164.520
45 CFR 164.530(i)
45 CFR 164.502(i)

The 2013 Final Rule changed the requirements for Notices of Privacy Practices. See Chapter 1, Section 2.A. for a discussion of the changes.

What is required:

Contents of the Notice. The dental practice must provide a Notice of Privacy Practices that contains certain required information. The 2013 HIPAA final rule changed the information required in the Notice, so existing Notices must be updated by September 23, 2013. The *Sample Notice of Privacy Practices* in Appendix 2.3.1 includes examples of the content required under the 2013 Final Rule. The NPP must be written in plain language.

Disabilities and LEP laws. A dental practice must comply with applicable federal and state laws that require the NPP to be accessible to patients with disabilities or limited English proficiency. For example, if a dental practice is required to comply with Title VI of the Civil Rights Act of 1964, it must take reasonable steps to ensure meaningful access for Limited English Proficient ("LEP") persons to the services of the dental practice, which could include translating the NPP into frequently encountered languages. Most covered entity dental practices are "public accommodations" under the Americans with Disabilities Act and must ensure effective communication with individuals with disabilities, which may require making the revised NPP available in alternate formats, such as Braille, large print, or audio.

Providing the Notice. The dental practice must provide the Notice to first-time patients at their first appointments, and ask the patient to sign an acknowledgment of receipt (see *Sample Acknowledgement of Receipt of Notice of Privacy Practices*, Appendix 2.3.2). If the patient declines to sign the acknowledgment, the practice must document that it attempted in good faith to obtain the acknowledgment, and note the reason why the acknowledgment was not obtained.

HIPAA permits, but does not require, providing the Notice and asking patients to sign the acknowledgement at every appointment. Some practices use this procedure to ensure that every patient has received the Notice.

Emergencies. In an emergency treatment situation, the dental practice must provide the Notice as soon as reasonably "practicable" (possible) after the emergency. A signed acknowledgment of receipt is not required.

Posting the notice; providing copies; website. The dental practice must also post the Notice in a clear and prominent location in the dental office and have copies of the Notice available at the dental office to hand out if someone asks for a copy to take with them. If the dental practice has a website that provides information about its customer services or benefits, it must prominently post the Notice on the website, and make the Notice available electronically through the website.

Email. A dental practice may only provide the Notice via email to people who have agreed to electronic notice, and who have not withdrawn that agreement (see *Sample Agreement to Receive Electronic Communication*, Appendix 2.22.3). If the dental practice knows that an email transmission failed, the practice must provide a paper copy of the Notice to the person.

Revising the Notice. The Notice must be revised as appropriate (for example, when the HIPAA rules change, or if the dental practice's privacy practices change). When a dental practice revises its Notice, the practice does not need to give the new Notice to patients who have already received the old Notice, nor ask those patients to sign a new acknowledgment form. Instead, on or after the effective date of the new Notice, the dental practice must (1) post the new Notice in a clear and prominent location in the dental office, (2) have copies available for people who request them, and (3) give a copy of the new Notice to anyone who asks for one. The revised Notice must also be posted on the dental practice's website, if applicable (see above). Signed Acknowledgment forms and each version of the Notice must be retained for at least six years from the date the document was created, or six years from the date the document last was in effect, whichever is later (Chapter 2, Step 19).

A dental practice that changes its Notice may not apply the changes to patient information that the dental practice had before the date of the change ***unless*** the Notice states that the dental practice reserves the right to change the terms of the Notice and to make the new terms effective for all patient information that the dental practice maintains, and the statement describes how the dental practice will provide individuals with a revised Notice.

Complying with the Notice. A dental practice may not use or disclose patient information in a way that is not consistent with its Notice of Privacy Practices.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our practice will provide a notice of our privacy practices to our patients, and to anyone else who requests a copy. Our Notice and the way we provide it will comply with HIPAA and applicable state law. Our practice will revise the Notice as appropriate, and will provide the revised Notice as required by HIPAA. Our practice will not use or disclose patient information in a manner that is inconsistent with our Notice, HIPAA, or state law.

Sample Procedures

Staff: Our Notice of Privacy Practices describes how our dental practice may use and disclose patient information. Ask the Privacy Official if you have any questions about the Notice. Do not use or disclose patient information in violation of our Notice.

Provide our Notice to each new patient at his or her first appointment, and ask the patient to sign the Acknowledgement of Receipt form (see *Sample Acknowledgement of Receipt of Notice of Privacy Practices*, Appendix 2.2). If a patient refuses to sign the acknowledgment of receipt, note on the form that you tried to get the acknowledgement, and the reason that you could not do so. If the patient has a personal representative, such as the parent or guardian of a minor, provide the Notice to the personal representative and ask the personal representative to sign the acknowledgement form.

Retain each completed acknowledgement form for six years from the date it was created or the date that it was last in effect, whichever is later. If we don't have an acknowledgment form for a patient, then at that patient's next appointment give the patient a copy of the Notice and ask the patient to sign the acknowledgement form.

SAMPLE POLICY AND PROCEDURES

We have a supply of Notices at the reception desk for people who ask for a copy to take with them. Give a copy to anyone who asks for one.

However, inmates do not have a right to a notice of privacy practices. An inmate is defined as a person who is incarcerated in or otherwise confined to a correctional institution.

Privacy Official: You are responsible for developing our Notice of Privacy Practices and for revising our Notice when appropriate – for example, if our privacy practices change, if the HIPAA rules change, or if there is a change in state law.

Providing the Notice. You are responsible for training workforce members to provide the Notice, for posting a copy of the Notice in a clear and prominent place in the dental office, for making sure there is a supply of Notices at the reception desk for people who ask for a copy to take with them, and for posting the Notice prominently on our practice's website and making it available electronically on our website.

Revising the Notice.

1. Whenever our privacy practices change, or there is a change in the law or the HIPAA Rules that requires a change to the Notice, determine whether our dental practice must revise the Notice. If so, revise the Notice as appropriate.
2. If our Notice is revised, then on or after the effective date of the revision, our practice will:
    a. Provide the new Notice to new patients on their first appointment and ask them to sign the acknowledgment.
    b. Have a supply of copies of the new Notice available in the dental office and give a copy to anyone who asks for a copy to take with them.
    c. Post the new Notice in a clear and prominent location in the dental office.
    d. Post the new Notice on our website, and make the new Notice available electronically through the website.
    e. Retain at least one copy of both the old and the new Notices for at least six years from the date when the document was created, or the date when the document last was in effect, whichever is later.

Complying with our Notice. Train workforce members to comply with our Notice.

Sample Forms:

- *Sample Notice of Privacy Practices*, Appendix 2.3.1
- *Sample Acknowledgment of Receipt of Notice of Privacy Practices*, Appendix 2.3.2

For more information:

Office for Civil Rights, *Notice of Privacy Practices for Protected Health Information*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html*

Appendix 2.3.1

Sample Notice of Privacy Practices

The sample Notice of Privacy Practices presents examples of the information that HIPAA requires a covered dental practice to give to patients concerning the dental practice's privacy practices. A dental practice should consult a qualified attorney in the appropriate jurisdiction to determine the provisions that need to be included in the Notice of Privacy Practices in order to reflect the dental practice's particular privacy policies and to comply with any applicable state laws.

{NAME OF PRACTICE}

Sample Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

We are required by law to maintain the privacy of protected health information, to provide individuals with notice of our legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information. We must follow the privacy practices that are described in this Notice while it is in effect. This Notice takes effect ____/____/____, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this Notice at any time, provided such changes are permitted by applicable law, and to make new Notice provisions effective for all protected health information that we maintain. When we make a significant change in our privacy practices, we will change this Notice and post the new Notice clearly and prominently at our practice location, and we will provide copies of the new Notice upon request.

You may request a copy of our Notice at any time. For more in formation about our privacy practices, or for additional copies of this Notice, please contact us using the information listed at the end of this Notice.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION ABOUT YOU

We may use and disclose your health information for different purposes, including treatment, payment, and health care operations. For each of these categories, we have provided a description and an example. Some information, such as HIV-related information, genetic information, alcohol and/or substance abuse records, and mental health records may be entitled to special confidentiality protections under applicable state or federal law. We will abide by these special protections as they pertain to applicable cases involving these types of records.

Treatment. We may use and disclose your health information for your treatment. For example, we may disclose your health information to a specialist providing treatment to you.

Payment. We may use and disclose your health information to obtain reimbursement for the treatment and services you receive from us or another entity involved with your care. Payment activities include billing, collections, claims management, and determinations of eligibility and coverage to obtain payment from you, an insurance company, or another third party. For example, we may send claims to your dental health plan containing certain health information.

Healthcare Operations. We may use and disclose your health information in connection with our healthcare operations. For example, healthcare operations include quality assessment and improvement activities, conducting training programs, and licensing activities.

Individuals Involved in Your Care or Payment for Your Care. We may disclose your health information to your family or friends or any other individual identified by you when they are involved in your care or in the payment for your care. Additionally, we may disclose information about you to a patient representative. If a person has the authority by law to make health care decisions for you, we will treat that patient representative the same way we would treat you with respect to your health information.

Disaster Relief. We may use or disclose your health information to assist in disaster relief efforts.

Required by Law. We may use or disclose your health information when we are required to do so by law.

Public Health Activities. We may disclose your health information for public health activities, including disclosures to:

- Prevent or control disease, injury or disability;
- Report child abuse or neglect;
- Report reactions to medications or problems with products or devices;
- Notify a person of a recall, repair, or replacement of products or devices;
- Notify a person who may have been exposed to a disease or condition; or
- Notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence.

National Security. We may disclose to military authorities the health information of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials health information required for lawful intelligence, counterintelligence, and other national security activities. We may disclose to correctional institution or law enforcement official having lawful custody the protected health information of an inmate or patient.

Secretary of HHS. We will disclose your health information to the Secretary of the U.S. Department of Health and Human Services when required to investigate or determine compliance with HIPAA.

Worker's Compensation. We may disclose your PHI to the extent authorized by and to the extent necessary to comply with laws relating to worker's compensation or other similar programs established by law.

Law Enforcement. We may disclose your PHI for law enforcement purposes as permitted by HIPAA, as required by law, or in response to a subpoena or court order.

Health Oversight Activities. We may disclose your PHI to an oversight agency for activities authorized by law. These oversight activities include audits, investigations, inspections, and credentialing, as necessary for licensure and for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Judicial and Administrative Proceedings. If you are involved in a lawsuit or a dispute, we may disclose your PHI in response to a court or administrative order. We may also disclose health information about you in response to a subpoena, discovery request, or other lawful process instituted by someone else involved in the dispute, but only if efforts have been made, either by the requesting party or us, to tell you about the request or to obtain an order protecting the information requested.

Research. We may disclose your PHI to researchers when their research has been approved by an institutional review board or privacy board that has reviewed the research proposal and established protocols to ensure the privacy of your information.

Coroners, Medical Examiners, and Funeral Directors. We may release your PHI to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also disclose PHI to funeral directors consistent with applicable law to enable them to carry out their duties.

Fundraising. We may contact you to provide you with information about our sponsored activities, including fundraising programs, as permitted by applicable law. If you do not wish to receive such information from us, you may opt out of receiving the communications.

OTHER USES AND DISCLOSURES OF PHI

Your authorization is required, with a few exceptions, for disclosure of psychotherapy notes, use or disclosure of PHI for marketing, and for the sale of PHI. We will also obtain your written authorization before using or disclosing your PHI for purposes other than those provided for in this Notice (or as otherwise permitted or required by law). You may revoke an authorization in writing at any time. Upon receipt of the written revocation, we will stop using or disclosing your PHI, except to the extent that we have already taken action in reliance on the authorization.

YOUR HEALTH INFORMATION RIGHTS

Access. You have the right to look at or get copies of your health information, with limited exceptions. You must make the request in writing. You may obtain a form to request access by using the contact information listed at the end of this Notice. You may also request access by sending us a letter to the address at the end of this Notice. If you request information that we maintain on paper, we may provide photocopies. If you request information that we maintain electronically, you have the right to an electronic copy. We will use the form and format you request if readily producible. We will charge you a reasonable cost-based fee for the cost of supplies and labor of copying, and for postage if you want copies mailed to you. Contact us using the information listed at the end of this Notice for an explanation of our fee structure.

If you are denied a request for access, you have the right to have the denial reviewed in accordance with the requirements of applicable law.

Disclosure Accounting. With the exception of certain disclosures, you have the right to receive an accounting of disclosures of your health information in accordance with applicable laws and regulations. To request an accounting of disclosures of your health information, you must submit your request in writing to the Privacy Official. If you request this accounting more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to the additional requests.

Right to Request a Restriction. You have the right to request additional restrictions on our use or disclosure of your PHI by submitting a written request to the Privacy Official. Your written request must include (1) what information you want to limit, (2) whether you want to limit our use, disclosure or both, and (3) to whom you want the limits to apply**. We are not required to agree to your request except in the case where the disclosure is to a health plan for purposes of carrying out payment** or health care operations, and the information pertains solely to a health care item or service for which you, or a person on your behalf (other than the health plan), has paid our practice in full.

Alternative Communication. You have the right to request that we communicate with you about your health information by alternative means or at alternative locations. You must make your request in writing. Your request must specify the alternative means or location, and provide satisfactory explanation of how payments will be handled under the alternative means or location you request. We will accommodate all reasonable requests. However, if we are unable to contact you using the ways or locations you have requested we may contact you using the information we have.

Amendment. You have the right to request that we amend your health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request under certain circumstances. If we agree to your request, we will amend your record(s) and notify you of such. If we deny your request for an amendment, we will provide you with a written explanation of why we denied it and explain your rights.

Right to Notification of a Breach. You will receive notifications of breaches of your unsecured protected health information as required by law.

Electronic Notice. You may receive a paper copy of this Notice upon request, even if you have agreed to receive this Notice electronically on our Web site or by electronic mail (email).

QUESTIONS AND COMPLAINTS

If you want more information about our privacy practices or have questions or concerns, please contact us.

If you are concerned that we may have violated your privacy rights, or if you disagree with a decision we made about access to your health information or in response to a request you made to amend or restrict the use or disclosure of your health information or to have us communicate with you by alternative means or at alternative locations, you may complain to us using the contact information listed at the end of this Notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to the privacy of your health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Our Privacy Official: _____

Telephone: _____ Fax: _____

Address: _____

Email: _____

Appendix 2.3.1b Sample Notice of Privacy Practices – Spanish Version

{NOMBRE DEL CONSULTORIO}

Ejemplo de un Aviso de Prácticas de Privacidad

ESTE AVISO DESCRIBE CÓMO SU INFORMACIÓN MÉDICA PUEDE SER USADA Y DIVULGADA Y CÓMO USTED PUEDE TENER ACCESO A ESTA INFORMACIÓN. POR FAVOR, LÉALO DETENIDAMENTE.

Por ley, a nosotros se nos requiere mantener la privacidad de la información de salud protegida, entregarles a los pacientes un aviso de nuestros deberes legales y prácticas de privacidad en lo que respecta a la información de salud protegida, y notificarles a las personas afectadas después de cualquier acceso no autorizado a la información de salud protegida. Nosotros tenemos que cumplir las prácticas de privacidad descritas en este Aviso mientras esté en vigencia. Este Aviso entrará en vigencia en ____/____/____, y seguirá vigente hasta que lo reemplacemos.

Nos reservamos el derecho a cambiar nuestras prácticas de privacidad y los términos de este Aviso en cualquier momento, siempre y cuando tales cambios estén permitidos por las leyes que correspondan, y para establecer la vigencia de disposiciones nuevas en el Aviso para toda la información de salud protegida que mantenemos. Cuando hagamos un cambio significativo en nuestras prácticas de privacidad, nosotros cambiaremos este Aviso, colocaremos una copia del Aviso nuevo de manera clara y prominente en nuestro consultorio y proporcionaremos copias del Aviso nuevo cuando sean solicitadas.

Usted puede pedir una copia de nuestro Aviso en cualquier momento. Para obtener más información sobre nuestras prácticas de privacidad o copias adicionales de este Aviso, comuníquese con nosotros usando la información de contacto al final de este Aviso.

MANERAS EN LAS QUE PODEMOS USAR Y DIVULGAR SU INFORMACIÓN DE SALUD

Nosotros podemos usar y divulgar su información de salud para diferentes propósitos, entre ellos tratamiento, pago y operaciones de salud. A continuación hemos proporcionado una descripción y un ejemplo de cada una de estas categorías. Cierta información, como por ejemplo la relacionada con VIH, genética, los expedientes de abuso de alcohol y/o substancias y los expedientes de salud mental podrían contar con protecciones especiales de confidencialidad de conformidad con las leyes estatales o federales correspondientes. Nosotros cumpliremos con estas protecciones especiales en lo que respecta a casos aplicables que incluyan estos tipos de expedientes.

Tratamiento. Nosotros podemos usar y divulgar su información de salud para su tratamiento. Por ejemplo, podemos compartir su información de salud con un especialista que le esté proporcionando tratamiento.

Pagos. Nosotros podemos usar y divulgar su información de salud para obtener reembolso por el tratamiento y los servicios que usted reciba de nosotros o de otra entidad involucrada en su atención. Las actividades de pago incluyen facturación, cobro, manejo de reclamos y determinaciones de elegibilidad y cobertura a fin de obtener pago de usted, una compañía de seguros o un tercero. Por ejemplo, podemos enviarle reclamos a su plan dental que contendrán cierta información de salud.

Operaciones de salud. Nosotros podemos usar y divulgar su información de salud en conexión con nuestras operaciones de salud. Por ejemplo, operaciones de salud incluyen evaluaciones de calidad y actividades de mejoramiento, conducir programas de capacitación y actividades de licenciamiento.

Personas involucradas en su atención o responsables de pagar por su atención. Nosotros podemos compartir su información de salud con un familiar o amigo suyo o con cualquier otra persona que usted identifique porque está involucrada con su atención o es responsable por el pago de su atención. Además, podemos divulgar información con respecto a usted con un representante de paciente. Si una persona cuenta con autorización legal para tomar decisiones de atención médica por usted, nosotros trataremos a ese representante del paciente de la misma manera que lo trataríamos a usted en lo que respecta a su información de salud.

Asistencia en caso de desastres. Nosotros podemos usar o divulgar su información de salud para prestar ayuda en casos de desastre.

Requerido por ley. Nosotros podemos usar o divulgar su información de salud cuando sea requerido por ley.

Actividades de salud pública. Nosotros podemos divulgar su información de salud por razones de salud pública, y estas incluyen:

- Prevenir o controlar enfermedades, lesiones o discapacidad;
- Reportar abuso de niños o casos de negligencia;
- Reportar reacciones a medicamentos o problemas con productos o aparatos;
- Notificarle a una persona sobre productos o aparatos que se van a recolectar, reparar o reemplazar;
- Notificarle a una persona que puede haber estado expuesta a una enfermedad o condición; o
- Notificarle a la autoridad gubernamental correspondiente cuando creamos que un paciente ha sido víctima de abuso, negligencia o violencia doméstica.

Seguridad Nacional. Nosotros podemos divulgarle la información de salud del personal de las fuerzas armadas a las autoridades militares en ciertas circunstancias. Nosotros podemos divulgarle a los funcionarios federales autorizados la información que requieran para actividades legales de inteligencia, contrainteligencia o de otro tipo de seguridad nacional. Nosotros podemos divulgarle la información de salud protegida de un recluso o paciente a una institución correccional u oficial de policía que tenga custodia legal de esa persona.

Secretario del Departamento de Salud y Servicios Humanos. Nosotros le divulgaremos su información de salud al Secretario del Departamento de Salud y Servicios Humanos de Estados Unidos cuando sea requerido para investigar o determinar el cumplimiento de la Ley HIPAA.

Compensación obrera. Nosotros podemos divulgar su información de salud protegida hasta el grado autorizado por y necesario para cumplir las leyes relacionadas con la compensación obrera u otros programas similares establecidos por ley.

Ejecución de la ley. Nosotros podemos divulgar su información de salud protegida por motivos de ejecución de la ley según esté permitido por la Ley HIPAA, como sea requerido legalmente, o en respuesta a un emplazamiento u orden de tribunal.

Actividades de supervisión de salud. Nosotros podemos compartir su información de salud protegida con una agencia de supervisión para actividades autorizadas por ley. Estas actividades de supervisión incluyen auditorías, investigaciones, inspecciones y determinaciones de credenciales según sean necesarias para obtener licencia y para que el gobierno supervise el sistema de atención médica, los programas gubernamentales y el cumplimiento de las leyes de derechos civiles.

Procesos judiciales y administrativos. Si usted está involucrado en una demanda o disputa, nosotros podemos divulgar su información de salud protegida en respuesta a una orden de un tribunal o administrativa. También podemos divulgar su información de salud en respuesta a un emplazamiento, solicitud de descubrimiento u otros procesos de ley instituidos por otra persona involucrada en la disputa, pero únicamente si han habido esfuerzos por la parte que la está solicitando o por nosotros de decirle sobre la solicitud o de obtener una orden para proteger la información solicitada.

Investigación. Nosotros podemos compartir su información de salud protegida con investigadores cuando su investigación haya sido aprobada por una junta de revisión institucional o junta de privacidad que haya revisado la propuesta de investigación y establecido protocolos para asegurar la privacidad de su información.

Médicos forenses y directores fúnebres. Nosotros podemos compartir su información de salud protegida con un médico forense. Esto podría ser necesario, por ejemplo, para identificar a una persona fallecida o determinar la causa de muerte. Nosotros también podemos compartir su información de salud protegida con directores fúnebres de conformidad con las leyes aplicables para que ellos puedan llevar a cabo sus funciones.

Recaudación de fondos. Nosotros podemos comunicarnos con usted para darle información sobre actividades que auspiciamos, que incluyen programas de recaudación de fondos, según lo permitan las leyes aplicables. Si usted no desea recibir ese tipo de información de nosotros, puede optar por no recibir las comunicaciones.

OTROS USOS Y DIVULGACIONES DE LA INFORMACIÓN DE SALUD PROTEGIDA

Se requerirá su autorización (con pocas excepciones) para divulgar notas de sicoterapia, usar o divulgar la información de salud protegida para propósitos de mercadeo o vender la información de salud protegida. Nosotros también obtendremos su autorización por escrito antes de usar o divulgar su información de salud protegida para propósitos que no sean los dispuestos en este Aviso (o como de otro modo lo permitan o requieran las leyes). Usted puede revocar una autorización por escrito en cualquier momento. Al recibir la revocación por escrito, nosotros dejaremos de usar o divulgar su información de salud protegida excepto al grado que ya hayamos tomado acción habiendo contado con la autorización.

SUS DERECHOS EN CUANTO A LA INFORMACIÓN DE SALUD

Acceso. Usted tiene derecho a ver o conseguir copias de su información de salud con limitadas excepciones. Usted deberá solicitarlo por escrito. El formulario para solicitar acceso se puede obtener usando la información de contacto al final de este Aviso. Usted también puede solicitar acceso enviándonos una carta a la dirección al final de este Aviso. Si solicita información que tenemos en papel, nosotros podemos proporcionarle fotocopias. Si pide información que mantenemos de forma electrónica, usted tiene derecho a obtener una copia electrónica. Nosotros usaremos la forma y formato que usted pida si está disponible. Nosotros le cobraremos un cargo razonable basado en el costo de los suministros y el trabajo de hacer las copias, y por el franqueo si quiere que le enviemos las copias por correo. Comuníquese con nosotros usando la información al final de este Aviso para que le expliquemos nuestra estructura de cargos.

Si se le niega una solicitud de acceso, usted tiene derecho a que la denegación sea revisada de conformidad con los requisitos de las leyes aplicables.

Registro de divulgación. Excepto en el caso de ciertas divulgaciones, usted tiene derecho a recibir un registro de las veces que se ha divulgado su información de salud de conformidad con las leyes y regulaciones aplicables. Para pedir un registro de las divulgaciones de su información de salud, deberá presentarle una solicitud por escrito al Funcionario de Privacidad. Si usted solicita este registro más de una vez en un período de 12 meses, nosotros podemos cobrarle un cargo razonable basado en el costo por responder a las solicitudes adicionales.

Derecho a solicitar una restricción. Usted tiene derecho de solicitar restricciones adicionales a nuestro uso o divulgación de su información de salud protegida presentándole una solicitud por escrito al Funcionario de Privacidad. Su solicitud por escrito deberá incluir (1) qué información desea limitar, (2) si desea limitar nuestro uso, divulgación, o ambos, y (3) a quién quiere que le apliquen las limitaciones. **A nosotros no se nos requiere estar de acuerdo con su solicitud excepto en el caso en que la divulgación sea a un plan médico con el propósito de recibir un pago** o efectuar operaciones de salud, y la información es únicamente en referencia a un artículo o servicio de salud por el que usted, o una persona a nombre suyo (que no sea el plan médico) le haya pagado por completo a nuestro consultorio.

Comunicación alternativa. Usted tiene derecho de solicitar que nos comuniquemos con usted sobre su información de salud por un medio alternativo o en un lugar alternativo. Usted deberá solicitarlo por escrito. Su solicitud deberá especificar el medio o lugar alternativo, y proporcionar una explicación satisfactoria sobre cómo se manejarán los pagos en el medio o lugar alternativo que está solicitando. Nosotros acomodaremos toda solicitud razonable. Sin embargo, si no podemos comunicarnos con usted usando los medios o lugares que ha solicitado, entonces podremos comunicarnos con usted usando la información que tengamos.

Enmienda. Usted tiene derecho a pedir que enmendemos su información de salud. Su solicitud deberá ser por escrito, y la misma deberá explicar por qué la información debe ser enmendada. Nosotros podemos denegar su solicitud en ciertas circunstancias. Si estamos de acuerdo con su solicitud, enmendaremos su expediente y se lo notificaremos. Si denegamos su solicitud de enmienda, le proporcionaremos una explicación por escrito de por qué la negamos y explicaremos sus derechos.

Derecho a recibir notificación de acceso no autorizado. Usted recibirá notificaciones de cualquier acceso no autorizado a su información de salud protegida según se requiere por ley.

Aviso electrónico. Usted puede recibir una copia impresa de este Aviso si la solicita, aún cuando haya acordado recibir este Aviso electrónicamente en nuestro sitio Web o por correo electrónico (e-mail).

PREGUNTAS Y QUEJAS

Si desea más información sobre nuestras prácticas de privacidad o tiene preguntas o inquietudes, comuníquese con nosotros.

Si le preocupa que pudiéramos haber violado sus derechos de privacidad, o si no está de acuerdo con una decisión nuestra en cuanto al acceso a su información de salud o en respuesta a una solicitud suya para enmendar o restringir el uso o divulgación de su información de salud o para que nos comuniquemos con usted por un medio alternativo o a un lugar alternativo, usted puede presentarnos una queja al respecto usando la información de contacto al final de este Aviso. Usted también puede presentarle una queja por escrito al Departamento de Salud y Servicios Humanos de Estados Unidos. Nosotros le proporcionaremos la dirección para presentar su queja ante el Departamento de Salud y Servicios Humanos de Estados Unidos cuando la solicite.

Nosotros apoyamos su derecho a la privacidad de su información de salud. Nosotros no tomaremos ningún tipo de represalia si usted decide presentarnos una queja a nosotros o ante el Departamento de Salud y Servicios Humanos de Estados Unidos.

Nuestro Funcionario de Privacidad: _____

Teléfono: _____ Fax: _____

Dirección: _____

Correo electrónico: _____

Appendix 2.3.2

Sample Acknowledgement of Receipt of Notice of Privacy Practices

This sample form illustrates how a dental practice might obtain acknowledgement of receipt of its Notice of Privacy Practices or document its good faith effort to obtain that acknowledgement.

{NAME OF PRACTICE}

You May Refuse to Sign This Acknowledgment

I have received a copy of this office's Notice of Privacy Practices.

Print Name: _____

Signature: _____

Date: _____

For Office Use Only

We attempted to obtain written acknowledgement of receipt of our Notice of Privacy Practices, but acknowledgement could not be obtained because:

- ☐ Individual refused to sign
- ☐ Communications barriers prohibited obtaining the acknowledgement
- ☐ An emergency situation prevented us from obtaining acknowledgement
- ☐ Other (Please Specify)

_____

_____

_____

Step 4: Designated Record Sets

Make a list of your "designated record sets."

Where to find the rules:

45 CFR 164.501
45 CFR 164.524
45 CFR 164.526

What is required:

A dental practice must create a list of the dental practice's "designated record sets" and retain the list for the time period required by HIPAA (Chapter 2, Step 19).

A dental practice's dental records and patient billing records are considered "designated record sets" under HIPAA.[3] A dental practice must also include on the list of designated record sets any other group of records used, in whole or in part, by the dental practice (or for the dental practice) to make decisions about patients. A "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.

Several of a patient's rights under HIPAA apply only to patient information in a "designated record set." For example, a patient has the right to:

- see information about the patient that the dental practice maintains in a designated record set, and/or get copies of information about the patient that the dental practice maintains in a designated record set (Chapter 2, Step 14.1), and
- have the dental practice amend, when appropriate, information or a record about the patient in a designated record set (Chapter 2, Step 14.2).

These rights apply for as long as the information is maintained in the designated record set.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our Privacy Official will create and retain a written list of our dental practice's "designated record sets," and will update the list whenever appropriate.

[3] Here is the official HIPAA definition of "designated record set," from 45 CFR § 164.501:
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.

Apéndice 2.3.2b

Ejemplo de acuse de recibo del Aviso de Prácticas de Privacidad

Este formulario de ejemplo ilustra cómo un consultorio odontológico puede obtener un acuse de recibo de su Aviso de Prácticas de Privacidad o documentar el esfuerzo realizado de buena fe para obtener ese acuse de recibo.

_____

{Nombre del consultorio}

Usted puede rehusarse a firmar este acuse de recibo

He recibido una copia del Aviso de Prácticas de Privacidad de este consultorio.

Nombre en letra de molde: _____

Firma: _____

Fecha: _____

Para uso interno solamente

Intentamos obtener un acuse de recibo por escrito de nuestro Aviso de Prácticas de Privacidad, pero no pudimos obtenerlo por el siguiente motivo:

- ☐ La persona se negó a firmar.
- ☐ Hubo barreras de comunicación que impidieron la obtención del acuse de recibo.
- ☐ Una situación de emergencia nos impidió obtener el acuse de recibo.
- ☐ Otro (especifique)

_____

_____

_____

SAMPLE POLICY AND PROCEDURES

Sample Procedures

Privacy Official: Create a list of every set of records in our dental practice that meets the HIPAA definition of a "designated record set" (see *Sample List of Designated Record Sets*, Appendix 2.4). The list must include: (1) all dental records and billing records about patients maintained by or for our dental practice, and (2) every group of records maintained by or for our dental practice that is used, in whole or in part, by or for our dental practice to make decisions about patients. Note that a "record" means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for our dental practice. Our designated record sets that are maintained off-site and/or by a business associate must be included on the list.

Whenever our dental practice changes its recordkeeping system in a way that changes our list of designated record sets, create a revised list of designated record sets. Retain each list for at least six years from the date when it was created, or from the date when it was last in effect, whichever is later.

ADA® TIP

To facilitate HIPAA compliance, the list of designated records sets may also include the following information:

- The date the list was created
- The date when the list was no longer in effect
- For each designated record set:
  - name of the record set
  - location (for example, whether the record set is maintained at the dental practice, or at the facility of a business associate such as an offsite storage facility)
  - whether the record set is maintained electronically or on paper (or both — for example, if records are kept in both formats, or if our practice is transitioning from paper to electronic), and
  - for electronic record sets only, the form(s) and format(s) of electronic copies that are readily producible, in case a patient requests an electronic copy of his or her records (Chapter 1 Section 2.E.2, Chapter 2 Step 14.1).

Sample Form:

- *Sample List of Designated Record Sets*, Appendix 2.4

Appendix 2.4
Sample List of Designated Record Sets

This sample form illustrates how a dental practice might write a list of designated record sets.

This list was created on_____ , 20 _____,

and was in effect until _____ , 20 _____.

Name of the record set	Location of the record set

Step 5: Minimum Necessary

Follow the "minimum necessary requirement" — Use, disclose, and request the minimum amount of patient information that is necessary for the intended purpose. Limit workforce access to patient information to the minimum necessary for their jobs. Have policies and procedures for routine uses, disclosures and requests, and assess the minimum necessary amount of patient information in non-routine situations. Respond appropriately to third party requests for patient information.

Where to find the rules:

45 CFR 164.502(b)
45 CFR 164.514(d)

Minimum necessary. When a dental practice uses or discloses patient information, or requests patient information from a health care provider, health plan, clearinghouse, or business associate, the dental practice must make reasonable efforts to limit the patient information to the minimum amount necessary to accomplish the intended purpose.

Exceptions: Minimum necessary does ***not*** apply in the following situations:

- Disclosing patient information to a health care provider for treatment purposes
- Requesting patient information from a health care provider for treatment purposes
- Disclosing a patient's information to the patient or personal representative
- When a patient has signed an authorization form for the use or disclosure (Chapter 2, Step 9)
- Disclosures to the U.S. Department of Health and Human Services ("HHS")
- Uses and disclosures required by law
- Uses and disclosures required in order to comply with the Privacy Rule

Entire dental record. A dental practice may not access, use, disclose or request a patient's entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure or request, or unless one of the above exceptions applies.

Business associates. Your dental practice's business associates must also make reasonable efforts to limit patient information to the minimum necessary for the purpose of the use, disclosure, or request. Depending on the terms of the business associate agreement (Chapter 2, Step 13) and the service that the business associate is providing to your dental practice, it may be necessary to provide your minimum necessary policies and procedures to a business associate.

Required steps. To comply with the minimum necessary requirement, a dental practice must take the following steps:

Step 5.1: Limit Workforce Access to Patient Information

Identify each workforce member or group (for example, dental assistants) in the dental practice that needs access to patient information to do their jobs. For each workforce member or group, indicate the category or categories of patient information that the person or group needs access to, and any conditions that may apply. Make reasonable efforts to limit each workforce members' access to the patient information to only that information which the workforce member need to do his or her job, and train the workforce not to access patient information for any other purpose. (see *Sample Workforce Access to Patient Information*, Appendix 2.5.1)

Step 5.2: Routine Disclosures and Requests

A dental practice makes certain routine disclosures of, and requests for, patient information. For routine disclosures and requests, the dental practice must have policies and procedures that limit the amount of information disclosed or requested to what is reasonably necessary for the purpose, and train staff to follow the procedures (see *Sample Routine Disclosures and Requests*, Appendix 2.5.2).

Step 5.3: Non-routine Disclosures and Requests

From time to time, a dental practice may wish to disclose or request patient information in a non-routine situation. A dental practice must assess non-routine disclosures and requests to determine the minimum amount of information that is necessary for the purpose.

Step 5.4: Minimum Necessary when Responding to Requests for Patient Information

In many cases a dental practice must determine the minimum necessary information to disclose when responding to an appropriate request for patient information, and may not rely on the person requesting the information to determine the minimum necessary amount. However, in the following situations, a dental practice **may** rely on the person making the request to determine the minimum necessary amount, when it is reasonable to do so under the circumstances:

- The dental practice is making a permitted disclosure to a public official and the public official tells the dental practice that the information requested is the minimum necessary for the stated purpose.
- A health care provider, health plan, or health care clearinghouse that is a HIPAA covered entity is asking for the patient information.
- A professional who is a member the dental practice's workforce, or who is a business associate of the dental practice, requests patient information in order to provide professional services to the dental practice, and the professional tells the dental practice that the information requested is the minimum necessary for the stated purpose.
- The dental practice wishes to disclose patient information for certain research purposes and the documentations and representations required in section 45 CFR 164.512(i) of the Privacy Rule are in place.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will use, disclose and request the minimum amount of patient information that is necessary for the intended purpose of the use, disclosure or request.

Sample Procedures

Staff: Do not access patient information that you are not authorized to access and is not necessary to do your job. Accessing patient information out of curiosity or for other impermissible purposes is prohibited, and will result in disciplinary action. When making a routine disclosure or request, follow our dental practice's written minimum necessary limits. Before our dental practice makes a non-routine disclosure or requests, we must assess the minimum necessary patient information for the purpose. Always limit uses, disclosures and requests for patient information to the minimum amount necessary for the purpose.

Privacy Official: Develop the following documents and keep them up to date:

- The minimum necessary patient information that our workforce members are authorized to access to do their jobs (see *Sample Workforce Access to Patient Information*, Appendix 2.5.1)
- Minimum necessary disclosures and requests in routine situations (see *Sample Routine Disclosures and Requests*, Appendix 2.5.2)

Assess non-routine disclosures and requests to determine the minimum necessary patient information for the purpose of the disclosure or request.

Train all workforce members to comply with the minimum necessary requirement.

Sample Forms:

- *Sample Workforce Access to Patient Information*, Appendix 2.5.1
- *Sample Routine Disclosures and Requests*, Appendix 2.5.2

For more information:

Office for Civil Rights, *Minimum Necessary Requirement*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html*.

Appendix 2.5.1

Sample Workforce Access to Patient Information

This sample form illustrates how a dental practice might document authorized workforce access to patient information.

This document was created on _____ , 20 _____,

and was in effect until _____ , 20 _____.

Name of workforce member or group	Patient information needed to do the job	Any conditions that apply to access

Appendix 2.5.2
Sample Routine Disclosures and Requests

This sample form illustrates how a dental practice might document minimum necessary levels for routine disclosures and requests.

For use when our dental practice makes a routine disclosure of patient information to a third party

This list was created on _____, 20 _____,
and was in effect until _____, 20 _____.

Type of routine disclosure	Patient information that may be disclosed without checking with the Privacy Official

For use when our dental practice makes a routine request for patient information from a third party

This list was created on _____, 20 _____,
and was in effect until _____, 20 _____.

Type of routine request for patient information	Patient information that may be requested without checking with the Privacy Official

Minimum necessary does not apply in the following situations:

- Disclosing patient information to a health care provider for treatment
- Requesting patient information from a health care provider for treatment
- Disclosing a patient's information to the patient
- When a patient has signed an authorization form for the use or disclosure
- Disclosures to the U.S. Department of Health and Human Services
- Uses and disclosures required by law
- Uses and disclosures required in order to comply with the Privacy Rule

Unless one of the above exceptions applies, our dental practice will not access, use, disclose or request a patient's entire dental record unless the entire dental record is needed to accomplish the purpose of the use, disclosure or request.

Step 6: Verify Identity

Verify identity when appropriate before disclosing patient information. A dental practice can violate HIPAA if an unauthorized person asks for patient information and the dental practice provides it without properly checking the person's identity and authority to get the information.

Where to find the rules:

45 CFR 164.514(h)

What is required:

When a person asks a dental practice for patient information, the dental practice must check to see who the person is and whether the person has the right to get the information requested, except:

- when the dental practice knows the person and knows that the person has the right to get the information
- disclosures requiring an opportunity for the patient to agree or object (Chapter 2, Step 8), as long as the dental practice exercises professional judgment in making the disclosure

Some disclosures require the dental practice to get certain documentation, statements, or representations. In these cases, the dental practice must get them *before* making the disclosure.

In the following situations, the dental practice should check the special rules in 45 CFR 164.514(h) for verifying identity, and consult an attorney when appropriate:

- before disclosing patient information to public officials
- administrative requests, subpoenas, or summonses, civil or authorized investigative demands, or similar processes
- disclosures for research

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will not disclose patient information to persons who do not have the authority to access the information.

Sample Procedures

Staff: If a person asks you for information about a patient, and you know the person and know that the person has the authority to get the information, you do not need to check the person's identity or authority.

If a person calls and asks you for patient information and you do not recognize the voice, verify the person's identity by asking for information such as date of birth, address, or approximate date of last appointment. If you are unsure, direct the request to the Privacy Official.

SAMPLE POLICY AND PROCEDURES

In all other cases, if a person asks for patient information and you do not know the person, or you are not sure that the person has the authority to access the information requested, direct the request to the Privacy Official who will verify the person's identity and authority to get the patient information requested.

Privacy Official: If a person asks for information about a patient, and we do not know the person and/or we are not sure that the person has the authority to access the information they asked for, you are responsible for verifying the person's identity and authority to get the patient information they request. You must also determine whether:

- the disclosure is required or permitted (Chapter 2, Steps 7 and 8),
- we need to have the patient sign an authorization form before our dental practice makes the disclosure (Chapter 2, Step 9 and *Sample Authorization Form for Use or Disclosure of Patient Information*, Appendix 2.9), and
- the minimum necessary information that may be disclosed, if applicable (Chapter 2, Step 5).

If a person we don't know comes to the dental office and asks for information about a patient, check the person's photo ID and any other appropriate documentation and do the following:

- If the person claims to be a patient asking for his or her own information, ask for date of birth, address, approximate date of last appointment, or some other information to verify identity. If the person wants to see or get copies of his or her own information, or a personal representative wants to see or get copies of the patient's information, see Chapter 2, Step 14.1.
- If the person says that he or she is a family member or friend of the patient, ask to see a photo ID and see Chapter 2, Step 6 about disclosures to friends or family members.
- If the person says that he or she is a patient's personal representative, ask to see a photo ID and exercise professional judgment to verify that the person is acting on behalf of the patient. Where appropriate, require the person to provide documentation, such as proof of legal guardianship or a Power of Attorney (see Chapter 2, Step 8 regarding disclosures to personal representatives).
- If the person is a public official, ask to see his or her identification badge or other credentials. If the request is in writing, review the government letterhead, insignia, address, and credentials.

If confronted with any of the following situations, check the special rules for verifying identity in 45 CFR 164.514(h) and consult legal counsel as appropriate:

- If a public official asks for patient information
- If the dental office receives an administrative request, subpoena, or summons, civil or authorized investigative demand, or similar process
- If the dental office receives a request for patient information for research purposes

SAMPLE POLICY AND PROCEDURES

If you have followed the verification procedures and you do not believe that our dental practice should provide patient information to the person asking for it, politely tell the person that we are unable to release the information. The person may submit a request in writing and provide more information about his or her identity and authority to get the information.

Require all persons, other than patients we know personally and their family members and friends as appropriate, (Chapter 2, Step 8) to complete the Verification of Identity Form (see *Sample Verification of Identity*, Appendix 2.6). Retain completed Verification of Identity Forms for six years from the date the document was created, or six years from the date the document was last in effect, whichever is later (Chapter 2, Step 19).

Sample Forms:

- *Sample Verification of Identity*, Appendix 2.6

Appendix 2.6

Sample Verification of Identity

This sample form illustrates how a dental practice might document the verification of the identity and authority of a person requesting patient information.

Please provide us with the following information.

Name of patient whose information you are requesting:

_____

Patient's Date of Birth: _____

The specific patient information that you are requesting: _____

_____

Your Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Describe your authority to access this information:

_____

If you are a patient's personal representative:

Relationship to Patient: _____

I certify that the above information is correct.

Signature: _____ Date: _____

Dental Staff: Describe documentation presented by the requester:

_____

Step 7: Required Disclosures

Understand which disclosures are required by HIPAA.

Where to find the rules:

45 CFR 164.502(a)(2)

What is required:

HIPAA requires a dental practice to disclose patient information in the following situations:

- When a patient (or a patient's personal representative) asks to see or get copies of the patient's information (Chapter 2, Step 14.1)
- When a patient (or a patient's personal representative) asks for an accounting of disclosures (Chapter 2, Step 14.3)
- When the U.S. Department of Health and Human Services ("HHS") requires patient information in order to investigate or determine the compliance with HIPAA.

In these situations, the dental practice does not need to have the patient sign an authorization form (Chapter 2, Step 9) before the dental practice makes the disclosure.

The minimum necessary requirement does not apply to these situations (Chapter 2, Step 5).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will disclose patient information when required by HIPAA.

Sample Procedures

Staff: Refer all of the following requests to the Privacy Official:

- If a patient, or a patient's personal representative, asks to see or get copies of the patient's information
- If a patient, or a patient's personal representative, asks for an accounting of disclosures
- If HHS asks for patient information

Privacy Official: HIPAA requires a dental practice to disclose patient information in response to an appropriate request from a patient or personal representative to see or get copies or for an accounting of disclosures. Disclosure is also required when patient information is requested by HHS in connection with a HIPAA investigation, compliance review, or audit. In these situations, patient authorization is not required, and the minimum necessary requirement does not apply. However, the steps outlined in Steps 14.1 and 14.3 must be followed as applicable.

Step 8: Permitted Uses and Disclosures

Understand when HIPAA permits a dental practice to use and disclose patient information without having the patient sign an authorization form.

A dental practice does not need to have a patient sign an authorization form (Chapter 2, Step 9) before the dental practice makes a "permitted" use or disclosure of the patient's information. However, the minimum necessary requirement applies to many permitted uses and disclosures (Chapter 2, Step 5), and if a business associate is involved, a business associate agreement must be in place (Chapter 2, Step 13).

> For example, disclosures for health care operations are permitted by HIPAA, so HIPAA does not require a dental practice to have the patient sign an authorization form (Chapter 2, Step 9) before the dental practice permits an auditing firm to access patient information. However, the dental practice may only disclose the minimum amount of patient information necessary for the audit (Chapter 2, Step 5), and the dental practice may require a business associate agreement with the auditing firm before permitting the firm to access patient information (Chapter 2, Step 13).

Many of the permitted uses and disclosures are complicated and contain specific requirements and limitations. A dental practice should refer to the HIPAA Rules and consult legal counsel before using or disclosing patient information without the patient's written authorization.

Sections 8.1 through 8.13 contain a ***simplified*** discussion of certain permitted uses and disclosures that are more likely to occur in a dental practice.

Section 8.14 contains a list of permitted uses and disclosures for which an authorization or opportunity to agree or object is not required, but no discussion of the requirements; for the specific requirements, see the applicable Privacy Rule provision. These uses and disclosures may occur less frequently in a dental practice and the rules that apply to these uses and disclosures are generally more complex.

8.1 **Permitted disclosures to the patient**

8.2 **Permitted uses and disclosures involving a personal representative, such as a parent or guardian**

8.3 **Permitted disclosures to a deceased patient's personal representative or others**

8.4 **Permitted uses and disclosures for Treatment Purposes**

8.5 **Permitted uses and disclosures for Payment Purposes**

8.6 **Permitted uses and disclosures for Health Care Operations Purposes**

8.7 **Permitted Incidental Uses and Disclosures**

8.8 **Permitted uses and disclosures in certain cases where the patient has the chance to agree or object**

8.9 **Permitted disclosures to a business associate**

8.10 **Permitted uses and disclosures involving whistleblowers**

8.11 **Permitted disclosures to a Law Enforcement Official**

8.12 **Permitted uses and disclosures concerning de-identification and limited data sets**

8.13 **Permitted uses and disclosures for fundraising**

8.14 **Permitted uses and disclosures for which an authorization or opportunity to agree or object is not required**

Step 8.1: Permitted disclosures to the patient

Where to find the rules:

45 CFR 164.502(a)(1)(i)

A dental practice may disclose patient information to the patient without having the patient sign an authorization form.

Step 8.2: Permitted uses and disclosures involving a personal representative, such as a parent or guardian

Where to find the rules:

45 CFR 164.502(g)
45 CFR 164.510(b)(5)

With certain exceptions, a dental practice must treat a patient's personal representative as the patient for purposes of HIPAA Privacy. In general, HIPAA permits a dental practice to disclose patient information to someone who has the right, under state or other applicable law, to make health care decisions for a patient as long as the patient information relates to the representation. However, there are exceptions. For example, a dental practice is not required to give a patient's information to the patient's personal representative if the dental practice has a reasonable belief that:

- the patient has been or may be subject to domestic violence, abuse or neglect by the personal representative, or
- giving information about the patient to the personal representative could endanger the patient, and
- the dental practice, in the exercise of professional judgment, decides that it is not in the patient's best interest to give the information to the personal representative.

For more information:

Office for Civil Rights, *Personal Representatives, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html*

Step 8.3: Permitted disclosures to a deceased patient's personal representative or others

Where to find the rules:

45 CFR 164.502(g)
45 CFR 164.510(b)(5)
45 CFR 164.502(f)

The 2013 Final Rule changed the requirements for disclosures of information about decedents. See Chapter 1, Section 2.H. for a discussion of the changes.

If a patient is deceased, the dental practice must treat the patient's executor, administrator, or other person who has the authority to act on behalf of the patient or the patient's estate as the patient's personal representative for HIPAA privacy purposes, with respect to patient information relevant to the personal representation.

However, a dental practice may disclose patient information to a family member, relative, close personal friend or other person, who was involved in the patient's care or payment for care, if the information is relevant to the person's involvement, unless doing so is inconsistent to a preference that the patient had expressed.

When appropriate, the dental practice should request proof of patient death, legal status of a personal representative, and familial relation.

Information about a patient who has been deceased for 50 or more years is no longer protected by HIPAA, although it may be protected by other applicable law or ethical rules.

Sample Decision Tree: Decedent PHI, Appendix 2.8, provides a sample decision tree tool to help understand permitted disclosures of decedents' information.

For more information about the rights of personal representatives see the Office for Civil Rights publication "Personal Representatives" *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalrepresentatives.pdf*

Step 8.4: Permitted uses and disclosures for Treatment Purposes

Where to find the rules:

45 CFR 164.501 (definition of "treatment")
45 CRF 164.502(a)(1)(ii)
45 CFR 164.506

HIPAA defines "treatment" to include:

- providing, coordinating and managing health care and related services by one or more health care providers, including coordination or management of health care by a health care provider with a third party,
- consultation between health care providers relating to a patient, and
- the referral of a patient for health care from one health care provider to another.

With certain exceptions, a dental practice may use or disclose patient information for the dental practice's treatment activities, and a dental practice may disclose patient information for the treatment activities of another health care provider, provided the use or disclosure is consistent with the other requirements of the HIPAA Privacy Rule.

Examples of the exceptions include psychotherapy notes (Chapter 2, Step 9), subsidized marketing communications (Chapter 2, Step 10), and sale of protected health information (Chapter 2, Step 11).

For more information:

Office for Civil Rights, *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html*.

Step 8.5: Permitted uses and disclosures for Payment Purposes

Where to find the rules:

45 FR 164.501 (definition of "payment")
45 CRF 164.502(a)(1)(ii)
45 FR 164.506

HIPAA defines "payment" to include a variety of activities, such as:

- a dental practice's activities to obtain reimbursement, including billing and collection activities
- a dental plan's activities to determine whether the plan is responsible for coverage, to provide coverage and benefits, and to provide reimbursement
- determinations of a patient's eligibility, review of medical necessity and appropriateness of care, and utilization review activities.

With certain exceptions, a dental practice may use or disclose patient information for its own payment activities, and may disclose patient information to another health care provider, or to a health plan or clearinghouse that is a HIPAA covered entity, for the payment activities of the provider, plan or clearinghouse, provided the use or disclosure is consistent with the other requirements of the HIPAA Privacy Rule.

Examples of the exceptions include psychotherapy notes (Chapter 2, Step 9), subsidized marketing communications (Chapter 2, Step 10), and sale of protected health information (Chapter 2, Step 11).

For more information:

Office for Civil Rights, *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html*.

Step 8.6: Permitted uses and disclosures for Health Care Operations Purposes

Where to find the rules:

45 FR 164.501 (definition of "health care operations")
45 CRF 164.502(a)(1)(ii)
45 FR 164.506

HIPAA defines "health care operations" to include a variety of activities, such as:

- business planning and development
- business management and general administrative activities
- sale of the dental practice to another HIPAA covered entity (or an entity that will become a covered entity after the sale) and due diligence related to the sale
- conducting or arranging for legal services, auditing functions, and medical review
- conducting quality assessment and improvement activities
- reviewing the competence or qualifications of health care professionals

- evaluating practitioner and provider performance
- conducting training programs for health care students, trainees or practitioners

With certain exceptions, a dental practice may use or disclose patient information for its own health care operations, or disclose patient information to a health care provider, health plan, or clearinghouse for their health care operations, provided the use or disclosure is consistent with the other requirements of the HIPAA Privacy Rule, and:

- the provider, plan or clearinghouse is a HIPAA covered entity
- the provider, plan or clearinghouse has or had a relationship with the patient
- the patient information pertains to that relationship, and
- the disclosure is for certain limited purposes, such as quality assessment and improvement, reviewing the competence or qualifications of health care professionals, or fraud and abuse detection or compliance.

Examples of the exceptions include psychotherapy notes (Chapter 2, Step 9), subsidized marketing communications (Chapter 2, Step 10), and sale of protected health information (Chapter 2, Step 11).

For more information:

Office for Civil Rights, *Uses and Disclosures for Treatment, Payment, and Health Care Operations*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html*.

Step 8.7: Permitted Incidental Uses and Disclosures

Where to find the rules:

45 CFR 164.502(a)(1)(iii)

What is required:

A dental practice does not need a patient to sign an authorization form (Chapter 2, Step 9) for a use or disclosure of patient information that is "incidental to" a use or disclosure that is permitted or required by HIPAA, provided the dental practice complies with the minimum necessary requirement (Chapter 2, Step 5) and has appropriate safeguards in place (Chapter 2, Step 20).

For example, a dentist may instruct the office manager to bill a patient for a particular procedure, and may be overheard by someone in the reception room. If the dentist made reasonable efforts to avoid being overheard and reasonably limited the information shared, the incidental disclosure to the person in the reception room is permissible under the Privacy Rule.

However, an incidental use or disclosure that occurs because a dental practice does not have reasonable safeguards or does not apply the minimum necessary standard where required is a violation of HIPAA. For example, if a dental practice permits an employee to have unimpeded access to patients' dental and billing records, where such access is not necessary for the employee to do his job, the incidental uses and disclosures that result may be unlawful under HIPAA.

For more information:

Office for Civil Rights, *Incidental Uses and Disclosures*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html*

Step 8.8: Permitted uses and disclosures in certain cases where the patient has the chance to agree or object

Where to find the rules:

45 CFR 164.510

In certain situations, a dental practice is not required to have a patient sign an authorization form (Chapter 2, Step 9) before the dental practice uses or discloses patient information if the patient:

- was told in advance about the use or disclosure, and
- had the opportunity to agree, prohibit or restrict the use or disclosure.

Examples of such permitted uses and disclosures include:

If the patient is present and has the capacity to make health care decisions, the dental practice may disclose the patient's information to the patient's family member, relative, close personal friend, or someone else identified by patient if:

- the information is directly relevant to the person's involvement with the patient's care or payment for care, and
- the dental practice either:
  - obtains the patient's agreement (this can be oral),
  - gives the patient the chance to object to the disclosure and the patient does not object, or
  - exercises professional judgment to reasonably infer from the circumstances that the patient does not object to the disclosure.

If the patient is not present, the dental practice may disclose patient information to a person involved in the patient's care or payment for care, if:

- the patient information is directly relevant to the person's involvement in the patient's care or payment for care, or is needed to notify a family member, personal representative, or other person responsible for the patient's care, and
- the dental practice exercises professional judgment and determines that the disclosure is in the patient's best interest.

A dental practice may allow a person to pick up a patient's filled prescription, medical supplies, x-rays, or similar forms of patient information if the dental practice uses professional judgment and its experience with common practice to make reasonable inferences of the patient's best interest in doing so.

For more information:

For more information about disclosures to patients' family members, friends, and other persons involved in a patient's care, see the Office for Civil Rights publication, "Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care," available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf*

Step 8.9: Permitted disclosures to a business associate

Where to find the rules:

45 CFR 164.502(e)

A dental practice does not need to have a patient sign an authorization form (Chapter 2, Step 9) before the dental practice discloses patient information to a business associate for a purpose permitted by HIPAA as long as a compliant written business associate agreement is in effect between the dental practice and the business associate. (Chapter 2, Step 13)

Step 8.10: Permitted uses and disclosures involving whistleblowers

Where to find the rules:

45 CFR 164.502(j)

A dental practice is not violation of HIPAA if a workforce member or business associate discloses patient information to a health oversight agency, public health authority, appropriate health care accreditation organization, or to an attorney, in certain situations.

The workforce member or business associate must believe in good faith that:

- the dental office has done something illegal, or something that violates professional or clinical standards, or
- the care, services, or conditions provided by the dental practice potentially endangers one or more patients, workers, or the public; and

The health oversight agency or public health authority must be authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the dental practice and the disclosure must be for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the dental practice.

A disclosure to an appropriate health care accreditation organization must be for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the dental practice.

A disclosure to an attorney must be to an attorney who was retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the dental practice's conduct described above.

Step 8.11: Permitted disclosures to a Law Enforcement Official

In addition to certain disclosures required by law, such as in response to a proper court-ordered warrant, subpoena or summons,[4] there are certain situations where a dental practice may disclose limited patient information in response to a request from a law enforcement official. Two of these situations are discussed below.

[4] 45 CFR 164.512(f)(1)

Step 8.11.1: Permitted disclosures for identifying or locating a suspect, fugitive, material witness or missing person

Where to find the rules:

45 CFR 164.512(f)(2)

Except for permitted disclosures required by law, a dental practice may disclose limited information about a patient in response to a law enforcement official's request for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. The dental practice may only disclose the following information:

(A) Name and address

(B) Date and place of birth

(C) Social Security number

(D) ABO blood type and rh factor

(E) Type of injury

(F) Date and time of treatment

(G) Date and time of death, if applicable, and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

In general, a dental practice may not disclose the following to a law enforcement official for purposes of location or identification: dental records, any patient information related to the patient's DNA or DNA analysis, or typing, samples or analysis of body fluids or tissue.

Step 8.11.2: Permitted disclosures when a workforce member is a crime victim

Where to find the rules:

45 CFR 164.502(j)

A dental practice is not in violation of HIPAA if a member of its workforce who is the victim of a criminal act discloses patient information to a law enforcement official, if:

- the patient information disclosed is about the suspected perpetrator of the criminal act; and
- the information disclosed is limited to the patient's:
  - Name and address;
  - Date and place of birth;
  - Social Security number;
  - ABO blood type and rh factor;
  - Type of injury;

- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Step 8.11.3: Other Permitted disclosures to law enforcement officials

In certain other situations that are not discussed above, a dental practice may disclose limited patient information in response to a request from a law enforcement official as long as the dental practice complies with the applicable HIPAA Privacy Rule provision and applicable state law. In general, these disclosures involve disclosures:

- as required by law
  - including laws that require the reporting of certain types of wounds or other physical injuries, with certain exceptions
  - in compliance with and as limited by the relevant requirements of a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer, a grand jury subpoena, or an administrative request, provided certain requirements are met[5]
- authorized by the victim of a crime,[6]
- about a death that may have resulted from criminal conduct,[7]
- of evidence of criminal activity on the dental practice's premises,[8] or
- to a law enforcement official in a medical emergency.[9]

A dental practice should refer to the relevant HIPAA Privacy Rule provisions and consult qualified legal counsel before disclosing patient information to a law enforcement official.

Step 8.12: Permitted uses and disclosures concerning de-identification and limited data sets

Where to find the rules:

45 CFR 164.502(d) (de-identification)
45 CFR 164.514(e) (limited data sets)

HIPAA permits a dental practice to use patient information to create de-identified information (Chapter 2, Step 21), or to disclose patient information only to a business associate for such purpose, whether or not the de-identified information is to be used by the dental practice.

HIPAA permits a dental practice to use or disclose a limited data set that meets the requirements of 45 CFR 164.514(e) if the dental practice enters into a compliant "data use agreement." Limited data sets and data use agreements are beyond the scope of this book, but dental practices should

[5] 45 CFR 164.512(f)(1)
[6] 45 CFR 164.512(f)(3)
[7] 45 CFR 164.512(f)(4)
[8] 45 CFR 164.512(f)(5)
[9] 45 CFR 164.512(f)(6)

understand that a limited data set is patient information that has almost all of the 18 HIPAA identifiers removed (Chapter 2, Step 21 and Chapter 3) except for certain date and location information, and that a limited data set may only be used for certain research, public health or health care operations purposes.

Properly de-identified patient information is not protected by HIPAA, and breach notification does not apply to properly de-identified patient information. However, a limited data set ***is*** protected by HIPAA, and following the impermissible use or disclosure of a limited data set, a dental practice must provide breach notification unless the dental practice can demonstrate a low probability of compromise based on a risk assessment that evaluates the relevant factors including the four required factors. (Chapter 2, Step 22).

A dental practice should consult qualified legal counsel before creating (or having a business associate create) a limited data set, or entering into a data use agreement.

Step 8.13: Permitted uses and disclosures for fundraising

Where to find the rules:

45 CFR 164.514(f)

Under certain circumstances, HIPAA permits a dental practice to use or disclose limited patient information to raise funds for the dental practice (see Chapter 2, Step 24 and Chapter 1, Section 2.K).

Step 8.14: Permitted uses and disclosures for which an authorization or opportunity to agree or object is not required

Where to find the rules:

45 CFR 164.512
45 CFR 164.514(e), (f)
45 CFR 164.502(d)

Each of the following permitted uses and disclosures involves detailed requirements that must be met prior to the use or disclosure. Review the requirements and consult qualified legal counsel prior to making these uses or disclosures of patient information to make sure all of the applicable requirements for the use or disclosure have been met.

- Uses and disclosures required by law 45 CFR 164.512(a)
- For public health activities,[10] such as:
    - Reporting disease and injury 45 CFR 164.512(b)(1)(i)
    - public health investigations 45 CFR 164.512(b)(1)(i)
    - reporting child abuse or neglect 45 CFR 164.512(b)(1)(ii)
    - reports involving FDA-regulated products or activities 45 CFR 164.512(b)(1)(iii)
    - disclosures regarding communicable diseases 45 CFR 164.512(b)(1)(iv)
    - disclosures regarding certain workers or work-related injuries or illness 45 CFR 164.512(b)(1)(v)

[10] For more information, see Office for Civil Rights, *Public Health, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html.*

- About victims of abuse, neglect or domestic violence 45 CFR 164.512(c)
- For certain health oversight activities 45 CFR 164.512(d)
- For judicial and administrative proceedings 45 CFR 164.512(e)
- For law enforcement purposes 45 CFR 164.512(f)
- To coroners, medical examiners and funeral directors 45 CFR 164.512(g)
- For organ donation purposes 45 CFR 164.512(h)
- For research purposes[11] 45 CFR 164.512(i)
- To avert a serious threat to health or safety 45 CFR 164.512(j)
- For specialized government functions, such as certain military and veterans activities, national security and intelligence activities, protective services for the President and others, and disclosures about inmates to correctional institutions or law enforcement officials 45 CFR 164.512(k)
- Disclosures for workers' compensation[12] 45 CFR 164.512(l)

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will not use or disclose patient information without written authorization unless the use or disclosure is required or permitted under HIPAA.

Sample Procedures

Staff: Do not use or disclose patient information, except for routine purposes that you are authorized and trained to make, unless you have the prior approval of the Privacy Official.

Privacy Official: You are responsible for determining whether a proposed use or disclosure of patient information requires the patient to sign an authorization form, or whether the use or disclosure is permitted or required by HIPAA.

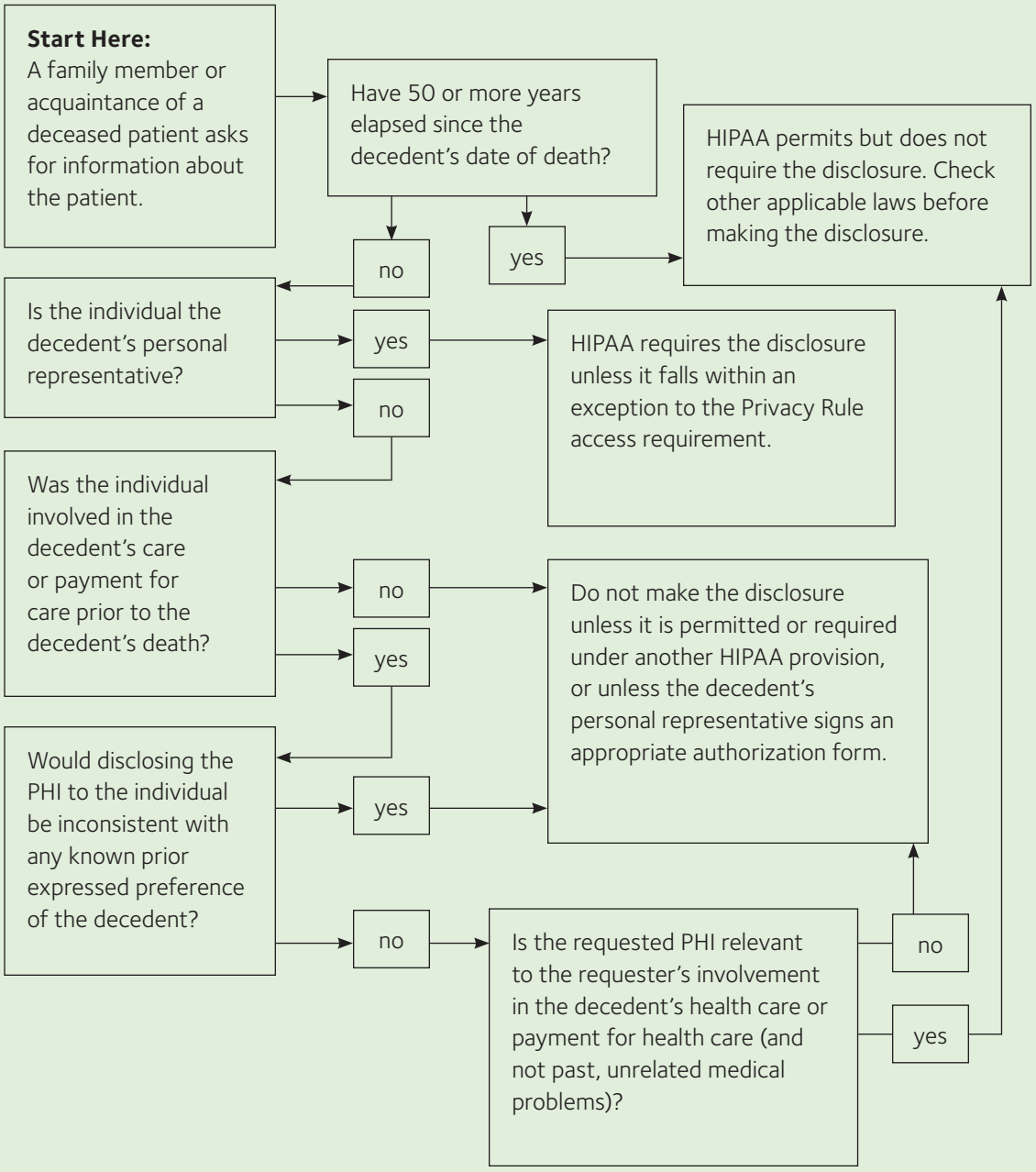
Develop policies and procedures for handling these situations that are likely to arise in our dental practice, train staff and put the policies and procedures into action.

Sample Forms:

- *Sample Decision Tree: Decedent PHI*, Appendix 2.8

[11] For more information, see Office for Civil Rights, *Research, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html.*
[12] For more information, see Office for Civil Rights, *Disclosures for Workers' Compensation Purposes, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/workerscomp.html.*

Appendix 2.8
Sample Decision Tree: Decedent PHI



Step 9: Patient Authorization Forms

Learn when a patient must sign an authorization form and what the form must say. Authorization forms must contain certain required information.

Where to find the rules:

45 CFR 164.508

What is required:

If a use or disclosure of patient information is not required or permitted by HIPAA (Chapter 2, Steps 7 and 8), a dental practice must have the patient sign an authorization form before the dental practice makes the use or disclosure. An authorization form must be in plain language and must contain certain required information. A dental practice may include additional information in the form as long as the additional information is not inconsistent with the required information. A sample authorization form, *Sample Authorization Form for Use or Disclosure of Patient Information*, is in Appendix 2.9.

In some cases, extra information must be in the authorization form. For example:

- Before a dental practice can use or disclose patient information for a subsidized marketing communication (Chapter 2, Step 10), the patient must sign an authorization form with the usual required information, plus a statement that the marketing involves "financial remuneration." Samples of authorization forms for subsidized marketing communications are in Appendices 2.10.1, 2.10.2 and 2.10.3.
- Before a dental practice can "sell" patient information (Chapter 2, Step 11), the patient must sign an authorization form with the usual information, plus a statement that the dental practice will receive "remuneration" (payment or something of value) in exchange for the patient information.

A signed authorization form only permits the dental practice to make the uses and disclosures authorized by the form. The patient is free to revoke (cancel) the authorization at any time, but must do so in writing. If the patient revokes the authorization, the dental practice has to stop the use or disclosure, but the revocation (cancelation) does not affect any uses and disclosures that the dental practice has already made in reliance on the authorization.

Compound and conditional authorizations. With certain exceptions, a dental practice may not combine an authorization form with any other document (this is called a "compound authorization"). With certain exceptions, a dental practice may not condition treatment, payment, enrollment in a health plan, or eligibility for benefits on whether or not the patient signs an authorization (this is referred to as a "conditional authorization"). If a dental practice wishes to have a patient sign a compound or conditional authorization, it should review the rules in 45 CFR 164.508(b)(3)–(4) and consult legal counsel to make sure the authorization falls into one of the exceptions.

Copy and documentation. When a patient signs an authorization form, the dental practice must give the patient a copy. The dental practice must keep each signed authorization form for at least six years from the date the document was created, or for at least six years from the date when the document was last in effect, whichever is later (Chapter 2, Step 19).

Consent forms. A "consent form" is not the same thing as a HIPAA "authorization form". HIPAA permits, but does not require, a dental practice to obtain a patient's consent for a use or disclosure that does not require authorization under HIPAA (for example, a use or disclosure for treatment,

payment or health care operations ("TPO"). A law other than HIPAA (for example, a state law) may require a dental practice to have a patient sign a consent form before the dental practice may disclose the patient's information for TPO purposes, or before the dental practice uses or discloses certain kinds of sensitive patient information, such as information about infection status (e.g., HIV), mental health, substance abuse, or genetics.

ADA® TIP

A dental practice would be prudent to give special protection to sensitive information like infection status, mental health, or substance abuse, in order to protect patient confidentiality and to protect the practice from liability. For example, if an inappropriate use or disclosure causes physical, financial, or reputational harm to the patient, or hindered the patient's ability to obtain health care, the government may impose more severe penalties.

In situations where HIPAA does require a signed authorization form, the form must meet all of the HIPAA requirements for the authorization form. A dental practice cannot use a consent form instead unless it meets the HIPAA requirements for an authorization form.

Information about consent forms is found in 45 CFR 164.506(b). A dental practice should consult qualified legal counsel to determine which uses and disclosures require consent under applicable law, develop appropriate forms, and train workforce members to obtain consent when appropriate. Consent forms required by state law should be retained for the appropriate period of time under HIPAA or applicable state law, whichever is longer.

Disclosures to schools. In general, before a dental practice discloses patient information about a student to a school, the dental practice must have a student's parent or guardian sign an authorization form (if the student is an adult or an emancipated minor, the student would need to sign the authorization form).

The 2013 Final Rule created an exception to the authorization requirement that applies only to disclosures of immunization records to schools (see Chapter 1, Section 2.I). A dental practice may rely on the parent or guardian's oral or written agreement to disclose proof of immunization to a school (or the student's agreement, in the case of an adult or emancipated minor). The dental practice must document the agreement; for example, by noting the information in the patient's chart, or if the agreement was in writing by placing the writing in the patient's chart. The rules on the simplified procedure for disclosing immunization records to schools are in 45 CFR 164.512((b)(1)(vi). A dental practice is not required to adopt the simplified procedure for disclosing immunization records to schools, and may require a written authorization instead.

Psychotherapy notes. Special rules apply to authorization forms for psychotherapy notes. Most dental practices do not have "psychotherapy notes," which means notes recorded by a mental health professional documenting or analyzing a counseling session. Psychotherapy notes do *not* include health history information provided by the patient concerning prescription drugs, treatment furnished to the patient, results of clinical tests, or a summary of diagnosis, functional status, treatment plan, symptoms, prognosis, progress to date, or counseling session start and stop times. If a dental practice has patient information that meets the definition of "psychotherapy notes," the practice should be aware that special rules apply to this kind of patient information. Rules pertaining to psychotherapy notes can be found at 45 CFR 164.508(a)(2) and (b)(3)-(4) and 45 CFR 164.524(a)(1)(i).

ADA TIP

Develop standard authorization forms that comply with HIPAA and applicable state law, and have them on hand for routine situations.

ADA TIP

Examples of uses and disclosures of patient information that require authorization include:

- Posting full face photos of patients on on the Internet.
- Using a patient's diagnostic photographs or radiographs to educate other patients, if the photographs or radiographs identify, or could be used to identify, the patient.
- Including identifiable patient information in an article.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our practice will not use or disclose patient information without having the patient sign an appropriate authorization form unless the Privacy Rule permits or requires the use or disclosure.

Sample Procedures

Staff: Consult the Privacy Official before using or disclosing patient information unless the use or disclosure is routine and you are authorized to make the use or disclosure.

Privacy Official. Train workforce members to recognize routine uses and disclosures that they are authorized to make and that are required or permitted by HIPAA, including uses and disclosures for purposes of treatment, payment and healthcare operations. If your state requires patient consent for certain uses and disclosures, train workforce members to use appropriate consent forms when required.

If the dental practice wishes to make a use or disclosure of patient information that is not permitted or required by HIPAA, the patient must first sign an authorization form.

Do the following four things when a signed authorization form is required:

1. Determine whether the dental practice's standard authorization form is sufficient, or whether additional information should be included on the form (for example, authorizations for subsidized marketing communication or for the sale of patient information require additional information in the form). Properly fill in all of appropriate the blanks on the form.

2. Verify identification if you do not personally know the person who will sign the authorization form, or if you are not sure the person is authorized to sign it (for example, if you are not sure that the person is a personal representative of a patient). Do not permit an unauthorized person to sign an authorization form.

SAMPLE POLICY AND PROCEDURES

3. Give the authorization form to the patient and let the patient read it and ask questions. Answer any questions the patient may have about the form. If the patient understands and agrees with the form, have the patient sign the form and return it to you.

4. Confirm that the authorization is properly completed and signed, and make sure that the following information is in the form:

- A description of the patient information to be used or disclosed
- The name of the person(s) authorized to make the use or disclosure
- The name of person(s) to whom the dental practice may disclosure the information
- The purpose for the use or disclosure (if the patient initiated the authorization you may write "at the request of the individual" in this space)
- An expiration date or an expiration event that relates to the patient or to the purpose of the use or disclosure
- Signature and date of signature of the patient or the patient's personal representative. If the authorization is signed by a patient's personal representative, the form must have a description of the representative's authority to act for the patient

Defective authorization. An authorization is defective and is not valid if:

- It has expired
- The required information has not been filled out completely
- Our practice knows that the authorization has been revoked
- It is an impermissible "compound authorization"
- It is an impermissible "conditional authorization"
- Our practice knows that material information in the authorization is false

5. Give the patient a copy of the completed, signed authorization form. Retain the authorization form for at least six years from the date of its creation, or from the date when it was last in effect, whichever is later.

Sample Forms:

- *Sample Authorization Form for Use and Disclosure of Patient Information*, Appendix 2.9

Appendix 2.9

Sample Authorization Form for Use or Disclosure of Patient Information

This sample form illustrates how a dental practice might obtain and document authorization for a use or disclosure of patient information that is not permitted or required by HIPAA.

Patient Name: _____

Patient's Date of Birth: _____ Patient's Chart No.: _____

I hereby authorize the use and disclosure of the patient information as described below. I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

Specific description of the patient information to be used or disclosed:

_____

_____

Purpose(s) of this use or disclosure: _____

[If the patient or the patient's personal representative is requesting the use or disclosure, you may write "at the request of the individual" for the purpose.]

I authorize the following person(s) to make this use or disclosure:

_____

_____

The following person(s) may receive this patient information:

_____

[If this authorization is required for a use or disclosure of patient information for a subsidized marketing communication, add "I understand that the dental practice will receive financial remuneration for making this marketing communication."]

[If this authorization is required for a sale of patient information, add "I understand that this disclosure will result in remuneration to the dental practice."]

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at _____ _____. **[Insert address of the Privacy Official (or other person at the dental office responsible for patient authorizations). If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]** If I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written revocation.

I understand that I may refuse to sign this authorization, and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits. **[If an exception to the prohibition on conditioning authorizations applies, delete this sentence and insert a description of the consequences to the patient of a refusal to sign the authorization.]**

This authorization expires on the following date, or when the following event occurs:

_____

[Expiration events must relate to the patient or to the purpose of the use or disclosure. If the authorization is for research, the expiration may state "end of the research study," "none," or similar language.]

Signature of Patient or Patient's Personal Representative:

_____Date:_____

If Personal Representative:

Print Name: _____

Signature:_____

Relationship to Patient: _____

_____

For Office Use Only

_____

Copy of signed authorization provided to the individual:

Date:_____

Initials: _____

Apéndice 2.9b

Ejemplo de formulario de autorización para el uso o la divulgación de información del paciente

Este formulario de ejemplo ilustra como un consultorio odontológico podría obtener y documentar una autorización para un uso o una divulgación de información del paciente que no están permitidos ni requeridos por HIPAA.

Nombre del paciente: _____

Fecha de nacimiento del paciente: _____

N.º de expediente del paciente:_____

Por el presente, autorizo el uso y la divulgación de la información del paciente según se describe a continuación. Entiendo que la información que se divulgue de conformidad con esta autorización puede estar sujeta a una nueva divulgación por parte del receptor y puede ya no estar protegida por los reglamentos de privacidad de la HIPAA.

Descripción específica de la información del paciente, que se va a utilizar o divulgar:

_____

_____

Propósito(s) de este uso o esta divulgación:_____

[Si el paciente o el representante personal del paciente está solicitando el uso o la divulgación, puede escribir "a petición de la persona" como propósito.]

Autorizo a la(s) siguiente(s) persona(s) a realizar este uso o esta divulgación:

_____

_____

Las siguientes personas pueden recibir esta información del paciente:

_____

[Si esta autorización se requiere para un uso o una divulgación de la información del paciente para una comunicación de marketing subsidiado, debe agregarse "Entiendo que el consultorio odontológico recibirá remuneración financiera por realizar esta comunicación de marketing"].

[Si esta autorización se requiere para una venta de la información del paciente, debe agregarse "Entiendo que esta divulgación dará lugar a una remuneración para el consultorio odontológico"].

Entiendo que puedo revocar esta autorización en cualquier momento, y que mi revocación no se hará efectiva a menos que sea por escrito y la haya recibido el funcionario de privacidad del consultorio en _____. **[Insertar el domicilio del funcionario de privacidad (o de la persona responsable de las autorizaciones de los pacientes del consultorio odontológico). Si la descripción de cómo revocar una autorización está en el Aviso de Prácticas de Privacidad, reemplace la primera frase de este párrafo con "Entiendo que puedo revocar esta autorización en cualquier momento siguiendo las instrucciones que figuran en el Aviso de Prácticas de Privacidad. Entiendo que mi revocación debe ser por escrito"].** Si revoco esta autorización, mi revocación no afectará ninguna acción tomada por el consultorio odontológico antes de recibir mi revocación por escrito.

Entiendo que puedo negarme a firmar esta autorización y que mi negativa a firmar no afectará de ninguna manera mi tratamiento, pago, inscripción en un plan de salud ni mi elegibilidad para recibir beneficios. **[Si corresponde una excepción a la prohibición de autorizaciones con condicionamientos, elimine esta oración e inserte una descripción de las consecuencias para el paciente si se niega a firmar la autorización].**

Esta autorización vence en la fecha indicada a continuación, o cuando ocurra el siguiente evento:

_____

[Los eventos de vencimiento deben estar relacionados con el paciente o con el propósito del uso y la divulgación. Si la autorización es para investigación, la fecha de vencimiento debe indicar "final del estudio de investigación", "ninguna", o un texto similar].

Firma del paciente o del representante personal del paciente:

_____Fecha: _____

Si es el representante personal:

Nombre en letra de molde: _____

Firma: _____

Relación con el paciente: _____

_____

PARA USO INTERNO SOLAMENTE

Se le entregó copia de la autorización firmada a la persona:

Fecha: _____

Iniciales: _____

Step 10: Subsidized Marketing Communications

With certain exceptions, 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 must have a patient sign an authorization form if the dental practice will use patient information (such as patient names and addresses, or information about a patient's dental condition) in order to make the marketing communication.

We will refer to such communications as "subsidized" marketing communications.

Where to find the rules:

45 CFR 164.501 (definition of "marketing")
45 CFR 164.508(a)(3)

The 2013 Final Rule changed the requirements for marketing communications. See Chapter 1, Section 2.F. for a discussion of the changes.

What is required:

A "marketing communication" is any kind of message that encourages the recipient to buy or use a product or service. In some cases, HIPAA permits a dental practice to make a marketing communication without patient authorization, as long as the communication is for a permissible purpose under HIPAA (such as treatment, case management, care coordination, or health plan benefits). For example:

- Face-to-face communications made by the dental practice to a patient or other individual (these must be in person, not by phone, email, etc.)
- Promotional gifts of nominal value provided by the dental practice[13]
- When the dental practice receives only non-financial or in-kind remuneration for making the communication
- Prescription refill reminders or other communications about a drug or biologic that is currently being prescribed to the person, but only if the payment received by the dental practice is reasonably related to the dental practice's cost of making the communication.

However, if an exception does not apply, a dental practice must have the patient sign an authorization form (Chapter 2, Step 9) before the dental practice or its business associate makes a subsidized marketing communication, and the authorization form must states that financial remuneration is involved (see the sample authorization forms listed at the end of this section). Authorization is also required if the marketing communication is not for a permissible purpose under HIPAA whether or not the dental practice receives financial remuneration.

[13] For example, dentists may give patients free toothbrushes, floss and toothpaste. 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.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Prior to making a marketing communication, our dental practice will obtain any required written authorization.

Sample Procedures

Staff: Unless approved, do not:

- Use or disclose patient information for making a communication that encourages someone to buy or use a product or service,
- Encourage patients to buy or use a product or service, or
- Accept payment from anyone for making a communication that encourages someone to buy or use a product or service.

Only the Dentist (or Practice Administrator) may approve subsidized marketing communications.

Privacy Official: Before the dental practice accepts financial remuneration (dollars) for making a communication encouraging someone to buy or use a product or service, or uses or discloses patient information for making such a communication, determine:

1. whether the communication meets the definition of a "marketing communication"
2. whether the communication is for a permissible purpose under HIPAA (such as treatment, case management, care coordination, or health plan benefits), and
3. whether the patient's written authorization is required

If patient authorization is required,

1. develop an appropriate authorization form that includes a statement that financial remuneration is involved, and
2. ensure that each patient signs the form before his or her information (including name and address) is used or disclosed for purposes of making the communication

If a patient revokes an authorization, ensure that the patient does not receive any further marketing communication.

In the following situations, a communication can be made without written authorization from the patient, even if the dental practice will receive financial remuneration, as long as the communication is for a permissible purpose under HIPAA:

- In-person face-to-face communications
- Promotional gifts of nominal value
- When the dental practice receives only non-financial or in-kind remuneration for making a communication for a permissible purpose under HIPAA
- Refill reminders or other communications about a drug or biologic that is currently being prescribed to the person, but only if the payment received by the dental practice is reasonably related to the dental practice's cost of making the communication

Sample Forms:

- *Sample Patient Authorization for Marketing — All Products and Services,* Appendix 2.10.1
- *Sample Patient Authorization for Marketing — Single Product or Service,* Appendix 2.10.2
- *Sample Patient Authorization for Marketing — Single Company,* Appendix 2.10.3

Appendix 2.10.1

Sample Patient Authorization for Marketing – All Products and Services

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications generally. The scope of an authorization may apply more narrowly to communications about a single product or service (see form 2.10.2), or to the products or services of a single company (see form 2.10.3). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

From time to time, our dental practice would like to tell patients about products and services that we think may be of interest to them.

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information about products and services from our dental practice, please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth: _____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me. I also authorize the dental practice to disclose such information to a business associate for purposes of sending marketing communications to me.

I understand that the dental practice receives financial remuneration for making marketing communications.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

I understand that if I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written revocation.

I understand that I may refuse to sign this authorization, and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.

This authorization expires on the following date, or when the following event occurs:

_____

Signature of Patient or Patient's Personal Representative:

_____Date: _____

If Personal Representative:

Print Name: _____

Signature:_____

Relationship to Patient: _____

_____

For Office Use Only

_____

Copy of signed authorization provided to the individual:

Date: _____

Initials:_____

Appendix 2.10.2

Sample Patient Authorization for Marketing – Single Product or Service

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications about a single product or service. The scope of an authorization may apply more broadly to the products or services of a single company (see form 2.10.3) or to marketing communications generally (see form 2.10.1). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

Our dental practice would like to tell our patients about a new product [or service] that we think may be of interest to them: _____ [insert name of product or service].

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information about this product [or service] from our dental practice, please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth:_____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me about the product or service described above. I also authorize the dental practice to disclose such information to a business associate for purposes of sending such marketing communications to me.

I understand that the dental practice will receive financial remuneration for making this marketing communication.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

I understand that if I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written revocation.

I understand that I may refuse to sign this authorization, and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.

This authorization expires on the following date, or when the following event occurs:

_____

Signature of Patient or Patient's Personal Representative:

_____Date: _____

If Personal Representative:

Print Name: _____

Signature:_____

Relationship to Patient: _____

_____

For Office Use Only

Copy of signed authorization provided to the individual:

Date: _____

Initials:_____

Appendix 2.10.3

Sample Patient Authorization for Marketing – Single Company

This sample form illustrates how a dental practice might obtain patient authorization for the use or disclosure of the patient's information for an appropriate subsidized marketing communication. The following authorization applies to subsidized communications about a single company's products and/or services. The scope of an authorization may apply more narrowly to a single product or service (see form 2.10.2) or more broadly to marketing communications generally (see form 2.10.1). Note that this sample form does not apply to the sale of patient information (Chapter 2, Step 11).

To our Patients:

Our dental practice would like to tell our patients about products [and/or services] from

_____

[insert name of company] that we think may be of interest to them.

When we give patients promotional gifts of nominal value, or recommend products or services in face-to-face communications, we do not require the patient's written authorization. However, we do require a patient's written authorization before sending other kinds of marketing communications if our dental practice receives financial remuneration for sending the communication.

If you would like to receive information from our dental practice about _____'s [insert name of company] products [and/or services], please complete and sign the authorization form below and return it to us at your convenience.

Authorization

Patient Name: _____

Patient's Date of Birth:_____ Patient's Chart No.: _____

I hereby authorize the dental practice to use my name and address and other information about my dental health to provide marketing communications to me about the products or services described above. I also authorize the dental practice to disclose such information to a business associate for purposes of sending such marketing communications to me.

I understand that the dental practice will receive financial remuneration for making this marketing communication.

I understand that information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by HIPAA Privacy regulations.

I understand that I may revoke this authorization at any time, and that my revocation is not effective unless it is in writing and received by the dental practice's Privacy Official at the following address:

_____

[If the description of how to revoke an authorization is in the Notice of Privacy Practice, replace the first sentence of this paragraph with "I understand that I may revoke this authorization at any time by following the directions in the Notice of Privacy Practices. I understand that my revocation must be in writing."]

If I revoke this authorization, my revocation will not affect any actions taken by the dental practice before receiving my written revocation.

I understand that I may refuse to sign this authorization, and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.

This authorization expires on the following date, or when the following event occurs:

_____

Signature of Patient or Patient's Personal Representative:

_____Date: _____

If Personal Representative

Print Name: _____

Signature:_____

Relationship to Patient: _____

_____

For Office Use Only

Copy of signed authorization provided to the individual:

Date: _____

Initials:_____

Step 11: Sale of Patient Information

Do not disclose patient information in exchange for "remuneration" (dollars or anything of value) from or on behalf of the recipient of the information without the patient's written authorization, unless an exception applies. The authorization form for the "sale" of patient information as defined by HIPAA must state that the dental practice will receive remuneration for the disclosure.

Where to find the rules:

45 CFR 164.502(a)(5)(ii)
45 CFR 164.508(a)(4)

The 2013 Final Rule changed the requirements for sale of patient information. See Chapter 1, Section 2.G for a discussion of the changes.

What is required:

In general, a dental practice must have a patient sign an authorization form (Chapter 2, Step 9) before disclosing the patient's information in exchange for "remuneration" (dollars or anything of value, whether financial, nonfinancial, or in-kind). This applies whether the dental practice or its business associate receives the remuneration, and whether the remuneration is received directly from the recipient of the information or is provided indirectly by someone else on behalf of the recipient. The authorization form must state that the disclosure will result in remuneration to the dental practice.

There are several exceptions to the definition of a "sale" of patient information (see Chapter 1, Section 2.G). The exceptions are located at 45 CFR 164.502(a)(5)(ii).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will not "sell" patient information (as defined by HIPAA) without the patient's written authorization.

Sample Procedures

Staff: You are prohibited from exchanging any information about our patients for money or anything else of value. "Information about our patients" includes patient lists, schedules, names and addresses, and any other information about our patients. "Anything of value" includes money, things, opportunities, information, or anything else that has even a small amount of value.

Privacy Official: Before the dental practice discloses patient information in exchange for anything of value, or permits a business associate to do so, you will determine whether the transaction would meet the definition of a "sale" of patient information in 45 CFR 164.502(a)(5)(ii).

If the transaction would be a "sale" as defined by HIPAA, ensure that our dental practice does not disclose patient information unless the patient has signed an authorization form that states that the practice will receive remuneration for the disclosure (see *Sample Authorization Form for Use or Disclosure of Patient Information*, Appendix 2.9). If a patient signs and then revokes the authorization form, ensure that no information about that patient is disclosed after the dental practice receives the revocation.

Step 12: Mitigate Harm

If a dental practice learns that patient information was used or disclosed improperly by the dental practice or by a business associate, the dental practice must do what it reasonably can to lessen any harm that the dental practice knows about.

Where to find the rules:

45 CFR 164.530(f)

What is required:

If a dental practice has used or disclosed, or uses or discloses patient information in violation of the dental practice's privacy policies and procedures, or in violation of the Privacy Rule, the dental practice must mitigate (lessen), to the extent practicable, any harmful effect that the dental practice knows about. A dental practice is also required to mitigate when one of the dental practice's business associate has inappropriately used or disclosed patient information.

SAMPLE POLICY AND PROCEDURES

Sample Policy

If our dental practice or one of our business associates uses or discloses patient information in violation of its privacy policies and procedures or in violation of the Privacy Rule, our dental practice will mitigate, to the extent practicable, any harmful effect known to us.

Sample Procedures

Staff: Immediately tell the Privacy Official about any improper use or disclosure of patient information by our dental practice or by one of our business associates. If you are aware of any harmful effects of the improper use or disclosure, or any ways to lessen those harmful effects, tell the Privacy Official immediately.

Privacy Official: When you discover that our dental practice or one of our business associates has used or disclosed patient information in violation of its policies and procedures, or in violation of the Privacy Rule:

- determine whether our dental practice is aware of any harmful effects of the use or disclosure
- If so, determine whether our dental practice is reasonably capable doing anything to lessen the harmful effects
- If so, see that our dental practice does so

Remember to comply with the Breach Notification Rule (Chapter 2, Step 22) and, if appropriate, log the use or disclosure in case the patient asks for an accounting of disclosures (Chapter 2, Step 14.3).

SAMPLE POLICY AND PROCEDURES

Also remember that if our dental practice knows that a business associate is doing something that violates the business associate agreement, you must:

- Determine whether it is a "material" breach of the agreement (for example, it is likely a material breach if a business associate that does not provide the dental practice timely notice of a breach of unsecured patient information).
- If the breach is material, our dental practice must plan and take reasonable steps to end the violation
- And, if those steps are not successful, terminate the agreement with the business associate, if it is "feasible" to do so (For example, it may not be "feasible" to end an agreement with a business associate at that time if there is not another person or company that could take over the business associate's responsibilities).

For more information:

There is a discussion of the mitigation requirement in OCR *Accountability*, at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf*.

Step 13: Business Associates

Identify your dental practice's business associates and sign a business associate agreement with each of them. The business associate agreement must contain the provisions required by HIPAA.

Where to find the rules:

45 CFR 160.103
45 CFR 164.502(e);
45 CFR 164.504(e)
45 CFR 164.308(b)
45 CFR 164.314(a)

The 2013 Final Rule changed the requirements for business associates. See Chapter 1, Section 2.C. for a discussion of the changes.

HIPAA defines a "business associate" to generally mean an outside person or entity that does a service for the dental practice that involves patient information. Examples include a billing service, document storage company, law firm, collection agency, or shredding firm that has access to patient information.

HIPAA does not permit a dental practice to let a business associate access patient information until the dental practice and the business associate have signed a written agreement containing certain required provisions. This agreement is called a "business associate agreement" (see *Sample Business Associate Agreement*, Appendix 2.13). Where a business associate agreement is not in place between the dental practice and a business associate, the dental practice is not compliant with HIPAA.

The 2013 Final Rule changed the provisions that must be included in a business associate agreement and expanded the definition of a business associate. Dental practices must revise their business associate agreements by the applicable compliance date, and must make sure they have business associate agreements in place with all persons and entities who meet the new definition of a business associate (Chapter 1, Section 2.C).

A dental practice does not need a business associate agreement with a health care provider that is treating the patient (e.g., a specialist, a dental lab, or a pharmacy), or with a dental plan for payment purposes. However, a dental practice must have a business associate agreement with a provider or plan that is acting as a business associate of the dental practice (for example, a dentist who is providing consulting services that involve access to patient information).

A business associate must comply with certain HIPAA requirements, and the federal government can investigate business associates and directly impose penalties on them for failure to comply with HIPAA. A business associate must have an agreement in place with each of its subcontractors that have access to patient information and the agreement must contain provisions required by HIPAA. The dental practice is not required to have an agreement with a subcontractor — that is the business associate's responsibility. However, a dental practice may, for example, require the business associate to notify the dental practice of any subcontractors who will have access to information about the dental practice's patients, or require a business associate to get the dental practice's approval before permitting a subcontractor to access patient information. The dental practice might withhold approval if, for example, the subcontractor doesn't appear to know that it must comply with HIPAA, if the subcontractor does not assure the dental practice that it is in compliance with HIPAA, or if there is not a written agreement between +the subcontractor and the business associate that complies with HIPAA.

To ensure that a business associate agreement is in place with each of a dental practice's business associates, a dental practice may wish to create a list of its business associates and the status of their business associate agreements.

A dental practice may be required to act if a business associate violates HIPAA (Chapter 2, Step 13.2, *What if a business associate violates HIPAA or the business associate agreement?*).

Some business associates may be deemed "agents" of the dental practice, which can increase the potential liability of the dental practice. For example, in some cases a dental practice can be liable for the business associate's HIPAA violations if the business associate is deemed an agent (Chapter 2, 13.3, *When a Business Associate is an Agent*).

Step 13.1: Who are your Dental Practice's Business Associates?

A person or entity becomes a business associate by:

- creating, receiving, maintaining (e.g., storing), or transmitting patient information for a dental practice,
- performing HIPAA functions or activities involving patient information for the dental practice, or
- providing services to the dental practice that involve patient information, such as legal, accounting, consulting, management, or financial services.

Certain technology companies may also be business associates of a dental practice. For example, companies that develop EHR software, billing and transcription applications, cloud service providers, and backup services companies may be business associates if they can access patient information. In addition, under the new HIPAA rule, business associates include:

- Health Information Exchange Organizations ("HIOs"), e-prescribing gateways, and other individuals or entities that provide data transmission services with respect to patient information to a dental practice and that require routine access to the patient information,
- Patient Safety Organizations ("PSOs"), and
- A personal health record ("PHR") vendor that a dental practice hires to provide PHR service to patients.

Subcontractors. If a business associate's subcontractor will have access to patient information, the subcontractor is also considered a HIPAA business associate, although the dental practice is not required to have a business associate agreement with a subcontractor (the business associate and the subcontractor must have a business associate agreement in place).

Workforce members. Workforce members are not a business associates and do not require a business associate agreement. A dental practice's "workforce" means its employees, volunteers, trainees, and other persons whose work for the dental practice is under the dental practice's *direct control*, whether or not they are paid by the dental practice.

Treatment. A dental practice does not need a business associate agreement with a health care provider when the dental gives the provider patient information for purposes of treating the patient (for example, when a dental practice gives patient information to a dental specialist or to a laboratory for treatment purposes).

Banks. A bank or financial institution is not a business associate when it processes payments (for example, by cashing checks or conducting funds transfers). However, a bank or financial institution may be a business associate if it performs functions above and beyond such payment processing activities, such as handling accounts receivables for a dental practice.

Insurance carriers. A dental practice does not need a business associate agreement with an insurance company when the dental practice buys a health plan or professional liability insurance. However, an insurance company might be a business associate relationship if the insurance company performing risk management activities or legal services involving patient information for the dental practice.

Conduits. Sometimes, a dental practice will ask a vendor to sign a business associate agreement and the vendor will say that it does not need to sign one because it is a "conduit." HIPAA has an exception for conduits, but it is narrow. Dental practices should carefully analyze whether a vendor fits into the exception before agreeing not to require a business associate agreement.

Under HIPAA, a person or entity is not a business associate if it acts as a "mere conduit" for the transportation of patient information but does not access the information other than on a random or infrequent basis as necessary to perform the transportation service or as required by law. Whether a person or entity is a mere conduit is a fact-specific determination based on the nature of the services provided and the extent to which the person or entity needs access to patient information to perform the service to the dental practice.

The conduit exception is intended to exclude only those persons and entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents.

Step 13.2: What if a Business Associate Violates HIPAA or the Business Associate Agreement?

If a dental practice knows that a business associate is in material violation of the business associate agreement, the dental practice must take certain steps. A dental practice that does not take these steps may be in violation of HIPAA. First, the dental practice must take reasonable steps to end the violation. If that is not successful, the dental practice has to terminate the business associate agreement, if that is feasible. A dental practice should also take reasonable steps to mitigate (lessen) any harm caused by the violation (Chapter 2, Step 12).

If a dental practice is unable to terminate a business associate agreement (for example, because there is no other viable business alternative) the dental practice would be prudent to develop a project plan to separate from a noncompliant business associate as soon as is reasonably possible.

Step 13.3: When a Business Associate is an Agent

A dental practice can be directly liable for the HIPAA violations of a business associate that is legally deemed to be an "agent" of the dental practice acting within the scope of the agency.

To decide whether a business associate is an agent, the government looks at the facts of each case. *The essential factor is whether the dental practice has the right or authority to control the business associate's conduct in the course of performing the service on behalf of the dental practice.*

Here are some factors that the federal government may look at to determine whether an agency relationship exists:

- Whether the dental practice had the authority to control or direct the business associate's conduct
- The time place, and purpose of the business associate's conduct
- Whether the business associate's service is commonly done by a business associate
- Whether or not the dental practice reasonably expected that a business associate would engage in the conduct in question
- The type of service and skill level required to perform the service (for example, a business associate is less likely to be an agent if a small dental practice hires the business associate to perform a task that a small practice is unlikely to have the expertise to perform for itself)
- Whether the dental practice is legally or otherwise prevented from performing the service or activity (e.g., accreditation)

Agents and the Breach Notification Rule.[14] Under the Breach Notification Rule (Chapter 2, Step 22) a business associate must report a breach of unsecured patient information to the dental practice without unreasonable delay, and in no event later than 60 days after the business associate discovers the breach. The dental practice must send breach notification without unreasonable delay and in no event later than 60 days after *receiving the report* from the business associate. Thus, in some cases, notice is timely up to ***120 days*** after the business associate discovered the breach.

However, if the business associate is an agent, the clock starts running for the dental practice on the date that the business associate agent discovered the breach, so the dental practice must send notice within ***60 days*** from the date the business associate agent discovered the breach. If a business associate agent takes too long to report a breach, or if the agent does not take reasonable steps to discover breaches, then *the dental practice* may be in violation of HIPAA. This is because the dental practice can be deemed to have "discovered" a breach on the date that a workforce member or agent knows of, or should reasonably have known of, the breach.

Agents and correcting HIPAA violations.[15] If a dental practice or business associate is in willful violation of HIPAA and does not correct the violation within 30 days, the federal government may impose a minimum $50,000 penalty. If a business associate agent is in willful violation of HIPAA, the federal government may "impute" (assign) the agent's knowledge of the violation to the dental practice for purposes of calculating the 30 day period. Thus, if the business associate agent is in willful violation of HIPAA for 30 days, and the dental practice learns of the violation on day 31 and corrects it right away, the dental practice might still face a fine under the highest penalty tier.

When negotiating a business associate agreement, a dental practice would be prudent to weigh the benefits of control over the business associate against the potential liability if the business associate is deemed an agent. If the business associate is likely to be deemed an agent, the dental practice would be prudent to conduct more rigorous due diligence and discuss with legal counsel whether to add certain provisions to the contract that may protect the dental practice, such as an indemnification provision, insurance requirements, or a statement of the scope of agency.

[14] For more information about the Breach Notification Rule, see Chapter 2, Step 22.
[15] For more information about HIPAA penalties, see Chapter 1, Sections 1.E and 2.J).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will manage our relationships with business associates in compliance with HIPAA, and will not permit a business associate to access patient information unless a compliant business associate agreement is in place.

Sample Procedures

Staff: Do not permit outside persons or entities, such as contractors, vendors and consultants, to access patient information unless the person or entity is not a HIPAA "business associate," or an appropriate business associate agreement is in place. In general, you may provide patient information to another health care provider for treatment purposes (for example, a specialist, dental lab, or pharmacy).

Notify the Privacy Official ***immediately*** if you have reason to suspect that a business associate agreement is required but not in place, or that a business associate may be in violation of HIPAA.

Privacy Official:

- Develop a Business Associate Agreement form for our dental practice to use, and update the form as appropriate (see *Sample Business Associate Agreement*, Appendix 2.13).
- Ensure that a compliant business associate agreement is in place for every business associate.

If our dental practice becomes aware that a business associate is in violation of HIPAA, then our practice must:

- Take reasonable steps to end the violation, and, if that is not successful,
- Determine whether it is feasible to terminate the business associate agreement
  - If feasible, terminate the agreement
  - If not feasible, develop a project plan for bringing the noncompliant business associate into compliance, or replacing the business associate as soon as is reasonably feasible
- Take reasonable steps to mitigate (lessen) any harm caused by the violation.

Sample Forms:

- *Sample Business Associate Agreement*, Appendix 2.13

For more information:

Office for Civil Rights, *Business Associates, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html*

Office for Civil Rights, *Business Associate Contracts, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html*

Appendix 2.13

Sample Business Associate Agreement

This sample form illustrates how a dental practice might enter into a business associate agreement with a business associate who will perform a service for the dental practice that involves access to patient information.

This sample business associate agreement is intended as only a tool to help dental practices comply with HIPAA. The sample provisions address only HIPAA requirements, not the underlying agreement between the parties, nor do these sample provisions address state law requirements. The sample may not be sufficient to create a binding contract under state law, and may not be compliant with applicable state law that is more stringent than HIPAA. Use of this sample agreement does not replace consultation with a lawyer or negotiations between the dental practice and business associate. Words or phrases contained in bold brackets (**[like this]**) are intended as optional language for dental practices using this sample agreement.

Sample Business Associate Agreement

This Business Associate Agreement (this "Agreement") is entered into as of

_____ , 20_____ , (the "Effective Date") by and between

_____ ("Dental Practice")

and _____("Business Associate").

RECITALS:

WHEREAS, Business Associate performs services for or on behalf of Dental Practice (the "Services") pursuant to that certain _____ Agreement dated _____, 20____ (the "Underlying Agreement"), which Services involve the access, use and/or disclosure of Protected Health Information (as defined below); and

WHEREAS, the parties desire to enter into this Agreement in order to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, as amended and in effect.

NOW THEREFORE, the parties agree as follows:

1. Definitions. Capitalized terms not otherwise defined in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Rule and Security Rule (as defined below).

(a) "Breach," when capitalized, shall have the meaning set forth in 45 CFR § 164.402 (including all of its subsections).

(b) "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, limited to information that Business Associate creates, accesses, receives or maintains for or on behalf of Dental Practice.

(c) "Protected Health Information" or "PHI" shall have the meaning set forth in in 45 CFR § 160.103, limited to information that Business Associate creates, accesses, receives or maintains for or on behalf of Dental Practice. PHI includes EPHI.

(d) "Privacy Rule" means the Standards for Privacy of Individually Identifiable Health Information, codified at 45 CFR parts 160 and 164, Subparts A, D and E, as currently in effect.

(e) "Security Rule" means the Standards for Security for the Protection of Electronic Protected Health Information, codified at 45 CFR parts 160 and 164, Subparts A and C, as currently in effect.

(f) "Unsecured Protected Health Information" shall have the same meaning as the term "unsecured protected health information" in 45 CFR § 164.402, limited to such information accessed, created, received or maintained by Business Associate.

2. Scope of Use and Disclosure of PHI.

(a) Business Associate Status. Business Associate acknowledges that it is Dental Practice's "business associate" as defined by HIPAA. Business Associate agrees to comply with the HIPAA regulations as they directly apply to business associates.

(b) Performance of Service. Business Associate shall not access, use or further disclose PHI other than as permitted or required by this Agreement, to perform the Services pursuant to the Underlying Agreement or as Required by Law. Business Associate shall not access, use or disclose PHI in any manner that would violate HIPAA if such access, use or disclosure was done by Dental Practice.

[1. Uses and Disclosures Permitted By Law. Business Associate may use or disclose PHI: (A) as is necessary for the proper management and administration of Business Associate's organization, and (B) to carry out the legal responsibilities of Business Associate; provided, however, that any permitted disclosure of PHI to a third party must be either Required By Law or subject to reasonable assurances obtained by Business Associate from the third party that PHI will be held confidentially, and securely, and used or disclosed only as Required By Law or for the purposes for which it was disclosed to such third party, and that any breaches of confidentiality of PHI which become known to such third party will be immediately reported to Business Associate.]

[2. Statistical Aggregation. Business Associate shall not use PHI for any compilation or aggregation of data or for any commercial purpose whatsoever not set forth in this Agreement, unless permitted by Dental Practice in a written document.]

[3. De-identification. Business Associate shall not use PHI to create de-identified PHI for any purpose not set forth in this Agreement, unless permitted by Dental Practice in a written document.]

(c) Minimum Necessary. Business Associate shall not access, use or disclose more than the minimum necessary PHI to perform or fulfill the intended permissible purpose, in accordance with this Agreement.

(d) Privacy Rule. To the extent Business Associate carries out one or more of Dental Practice's obligations under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of HIPAA that apply to Dental Practice in the performance of such obligation(s).

(e) Security Rule and Safeguards. Business Associate shall use safeguards that are appropriate and sufficient to prevent access, use or disclosure of PHI other than as permitted or required by this Agreement. Business Associate shall comply with the Security Rule with respect to EPHI, including implementing Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity and Availability of EPHI.

(f) Notification. Without unreasonable delay, Business Associate shall notify Dental Practice, in writing, of any use or disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware. Without unreasonable delay, Business Associate shall report to Dental Practice in writing of any Security Incident of which it becomes aware in accordance with the Security Rule and Business Associate's obligations under the same. Upon Dental Practice's request, Business Associate shall provide a report of any and all impermissible uses, disclosures and/or Security Incidents.

(g) Subcontractors. Business Associate shall ensure that any and all subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree, in writing, to the same restrictions and conditions that apply to Business Associate. Each subcontract agreement must include, without limitation, the provisions of this Agreement. Business Associate shall make such agreements with its subcontractors available to Dental Practice upon request.

(h) Audit. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Dental Practice available to the Secretary of Health and Human Services and/or Dental Practice, upon request, for purposes of determining and facilitating Dental Practice's compliance with HIPAA.

(i) Patient Rights.

1. Patient Right to Review. Business Associate shall make PHI maintained in a Designated Record Set available to Dental Practice or, at the direction of Dental Practice, to an Individual, in accordance with §164.524 of the Privacy Rule.

2. Patient Right to Amend. Business Associate shall make PHI available for amendment and incorporate any amendments to PHI maintained in a Designated Record Set at the direction of Dental Practice and in accordance with §164.526 of the Privacy Rule. Dental Practice shall be involved in any decision of Business Associate to amend the PHI of an Individual.

3. Patient Right to Request Accounting. Business Associate shall document and make available to Dental Practice or, at the direction of Dental Practice, to an Individual, information relating to such Individual as is necessary for Dental Practice to respond to a request for an accounting of disclosures in accordance with §164.528 of the Privacy Rule.

   A. Business Associate agrees to implement an appropriate record-keeping process to ensure compliance with the requirements of this Section.

   B. Business Associate agrees to provide PHI it maintains electronically in a Designated Record Set in an electronic form at the request of Dental Practice or an Individual.

4. Notice to Dental Practice. Business Associate shall notify Dental Practice immediately in writing upon receiving a request from an Individual to review, copy or amend his or her medical record information or to receive an accounting of disclosures. Business Associate shall also provide Dental Practice with a prompt written report of the details of its handling of such requests.

(j) Breach. Business Associate shall notify Dental Practice of breaches of unsecured PHI in accordance with the requirements of 45 CFR § 164.410. Such notification shall include, to the extent possible, the identification of each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed during the Breach, along with any other information that Dental Practice will be required to include in its notification to an affected Individual, the media and/or the Secretary, as applicable, including, without limitation, a description of the Breach, the date of the Breach and its discovery, the types of Unsecured Protected Health Information involved and a description of Business Associate's investigation, mitigation and prevention efforts.

(k) Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or a subcontractor or agent of Business Associate in violation of the requirements of this Agreement, the Privacy Rule, the Security Rule or other applicable federal or state law.

3. [Dental Practice Obligations.]

[(a) Notice of Privacy Practices. Dental Practice shall notify Business Associate of limitation(s) in its notice of privacy practices to the extent such limitation affects Business Associate's permitted uses or disclosures under this Agreement.]

[(b) Individual Authorization. Dental Practice shall notify Business Associate of changes in, or revocation of, authorization by an Individual to use or disclose PHI, to the extent such changes affect Business Associate's permitted uses or disclosures under this Agreement.]

[(c) Restrictions. Dental Practice shall notify Business Associate of restriction(s) in the use or disclosure of PHI that Dental Practice has agreed to, to the extent such restriction affects Business Associate's permitted uses or disclosures under this Agreement.]

4. Term and Termination.

(a) Term. The Term of this Agreement shall become effective as of the Effective Date, and remain in effect until all PHI is returned or destroyed in accordance with this Section.

(b) Termination for Cause. Dental Practice may terminate this Agreement immediately if Dental Practice, in its sole discretion, determines that Business Associate has violated a material term of this Agreement. Dental Practice, at its option and within its sole discretion, may (1) permit Business Associate take steps to cure the breach; and (2) in the event Dental Practice determines such cure is sufficient, elect to keep this Agreement in force.

(c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall promptly return to Dental Practice or destroy all PHI received from Dental Practice, or created or received by Business Associate on behalf of Dental Practice, that Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI in any form. Upon request by Dental Practice, Business Associate shall promptly supply a certification executed by an officer (vice president level or above) of the Business Associate confirming that Business Associate has returned or destroyed all PHI and all copies thereof.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

5. [Limitation of Liability, Indemnification and Insurance.]

[(a) Limitation of Liability. To the extent that Business Associate has limited its liability under the terms of the Underlying Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect or punitive damages, or other such limitations, all limitations shall exclude damages to Dental Practice arising out of a breach of this Agreement by Business Associate or any Breach of PHI by Business Associate.]

[(b) Indemnification. Business Associate agrees to indemnify, defend, and hold harmless Dental Practice and its directors, officers, affiliates, employees, agents, and permitted successors from and against any and all claims, losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or related to Business Associate's breach of its obligations under this Agreement, including, but not limited to a Breach of Unsecured Protected Health Information by Business Associate.]

[(c) Insurance. Business Associate agrees at the request of Dental Practice, to obtain and maintain insurance coverage against the improper use and disclosure of PHI by Business Associate, naming Dental Practice as a named insured. Promptly following a request by Dental Practice for the maintenance of such insurance coverage, Business Associate will provide a certificate evidencing such insurance coverage.]

6. Miscellaneous Provisions.

(a) Notices. Any notice required or permitted under this Agreement will be given in writing and will be sent —

to Dental Practice at: _____
_____
_____

to Business Associate at: _____
_____
_____

Notices will be deemed to have been received upon actual receipt, one business day after being sent by overnight courier service, or three business days after mailing by first-class mail, whichever occurs first.

(b) Governing Law. This Agreement will be governed by, and construed in accordance with the laws of the state of [STATE] without giving effect to choice of law provisions thereof.

(c) Waiver. No delay or omission by either party to exercise any right or remedy under this Agreement will be construed to be either acquiescence or the waiver of the ability to exercise any right or remedy in the future. Failure of a party to insist upon strict adherence to any term or condition of this Agreement shall not be considered a waiver by that party of its right thereafter to insist upon strict adherence to that, or any other, term or condition of this Agreement. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof, and no waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

(d) Severability. All provisions of this Agreement are separate and divisible, and if any part or parts of this Agreement are held to be unenforceable, the remainder of this Agreement will continue in full force and effect.

(e) Amendments. The parties shall amend this Agreement from time to time by mutual written agreement in order to keep this Agreement consistent with any changes made to the HIPAA laws or regulations in effect as of the Effective Date and with any new regulations promulgated under HIPAA. Dental Practice may terminate this Agreement and, where appropriate, the Underlying Agreement in whole or in part if the parties are unable to agree to such changes by the compliance date for such new or revised HIPAA laws or regulations.

(f) Interpretation. In the event of any conflict between the provisions of this Agreement and the Underlying Agreement, the provisions of this Agreement shall control. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA.

(g) Automatic Amendment. This Agreement shall automatically incorporate any change or modification of applicable state or federal law as of the effective date of the change or modification. Business Associate agrees to maintain compliance with all changes or modifications to applicable state or federal law.

(h Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

(i) Independent contractor. The parties acknowledge and agree that Business Associate is an independent contractor. Nothing in this agreement shall be construed to create any partnership, joint venture, agency, or employment relationship of any kind between the parties. Notwithstanding the foregoing, to the extent that Business Associate is ever determined for any purpose to be an agent of the Dental Practice (under the Federal common law of agency or otherwise), Business Associate shall be acting outside of the scope of agency if Business Associate fails to notify the Dental Practice immediately if Business Associate violates or breaches any provision of this Agreement or violates the HIPAA Rules.

IN WITNESS WHEREOF, the parties have executed this Business Associate Agreement as of the Effective Date.

DENTAL PRACTICE	**BUSINESS ASSOCIATE**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

Step 14: Patient Rights and Requests

Respond appropriately when a patient (or a patient's personal representative[16]) makes a request involving patient information.

What is required:

HIPAA gives patients certain rights. Each of these rights has specific limitations. When a patient attempts to exercise one of these rights, HIPAA requires a dental practice to take certain steps.

Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

HIPAA gives patients the right to:

- See and get copies of their patient information: **14.1 Access**
- Ask the dental practice to make changes in their patient information: **14.2 Amendment**
- Get an accounting of certain disclosures of their patient information: **14.3 Accounting of Disclosures**
- Ask the dental practice to communicate with the patient in a different way or at a different location: **14.4 Confidential Communications**
- Ask the dental practice not to disclose his or her patient information: **14.5 Restricted Disclosure**

Each of these rights is discussed below. Patients do not need to sign an authorization form to exercise these rights, although in some cases a request must be made in writing or the dental practice must create documentation.

Keep in mind that when someone attempts to exercise a HIPAA right, the dental practice should verify identity where appropriate (Chapter 2, Step 6).

For an explanation of patient rights under HIPAA from the patient's perspective, see Office for Civil Rights, *Your Medical Records*, at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/medicalrecords.html*

[16] For information about patients' personal representatives, see Step 8. The U.S. Department of Health and Human Services provides information about personal representatives at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/personalreps.html*.

Step 14.1: Access

When a patient asks to see or get a copy of the patient's information in a designated record set.

Note: Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

Where to find the rules:

45 CFR 164.524

The 2013 Final Rule changed the requirements for patient access to records. See Chapter 1, Section 2.E. for a discussion of the changes.

What is required:

A dental practice must create a list of the dental practice's "designated record sets" (Chapter 2, Step 4), and must permit patients to make the following requests concerning information about the patient that the dental practice maintains in a designated record set:

- To see the information
- To get copies of the information
- To both see and get copies of the information

These requests are called requests for "access." A dental practice must respond to such requests appropriately and in a timely manner (see below). In most cases the dental practice will provide the requested access, but in some limited situations HIPAA permits a dental practice to deny the request (see "Denying the Request" below).

A request for copies may require the dental practice to ***send*** the copies to the patient or to a third party designated by the patient.

Keep in mind that HIPAA does not preempt more stringent state laws, so a dental practice must also comply with applicable state law that, for example, requires the dental practice to respond in a shorter timeframe than HIPAA requires, or to charge a lower fee for copies than HIPAA permits.

Verify identity. The Privacy Rule requires dental practices to have reasonable policies and procedures to verify the identity of any person who requests patient information, as well as the authority of the person to have access to the information, if the identity or authority of the person is not already known (Chapter 2, Step 6). A dental practice must not permit a person to access patient information if the person does not provide sufficient verification of his or her identity and authority to access the information requested.

Written request. If a patient asks the dental practice to send his or her information to someone else, the request must be in writing, signed by the patient, and clearly identify the designated person and where to send the copy (see "Requests to provide an electronic copy to someone else," below).

HIPAA permits a dental practice to determine whether to accept oral requests to see or get copies of information, or to require that requests be made in writing (as long as the dental practice has informed people they must submit requests in writing).

ADA TIP

A dental practice would be prudent to require requests for access to be in writing so that the details of the request are clear and the dental practice can easily determine the timeframe for responding to the request. In addition, if a patient asks the dental practice to email unencrypted copies of records, the dental practice must notify the patient that there is a risk that the information in the email could be read by a third party. A dental practice that requires requests for access to be in writing can provide this notice in the request form (see *Sample Request for Access*, Appendix 2.14.1). A dental practice that correctly enters the email address provided by the patient is not responsible for email while in transit or after the patient receives it.

Timeframe. When a patient asks to see or get copies of information, the dental practice has up to **30 days** to respond. The Privacy Rule establishes the 30 days as an outside limit, but a dental practice may respond sooner. The 30 day period starts running on the day the dental practice receives the request. To respond to a request, the dental practice must do one of the following three things:

1. ***Grant the request.*** If the dental practice does not have appropriate grounds to deny the request, the dental practice must tell the patient that the dental practice will grant the request, and then fulfill the request in the way that HIPAA requires (see below).

2. ***Deny the request.*** If the dental practice has appropriate grounds to deny the request, the dental practice must give the patient a written denial (see below).

3. ***Extend the time.*** If the dental practice cannot either grant or deny the request within the 30 day period, the dental practice may extend the time by up to 30 additional days as long as the dental practice gives the patient a written statement that states the reasons for the delay and the date by which the dental practice will complete its action on the request. A dental practice can only have one such 30-day extension. Before the end of the extension the dental practice must grant or deny the request.

Granting the Request.
If a dental practice grants the request, the dental practice must let patients see the information (if that is what they asked for), or get copies (if that is what they asked for). If a patient asks both to see and get copies, the dental practice must provide both.

Form and Format. In general, the dental practice must let the patient see or get copies in the form and format that the patient asked for, if the dental practice can reasonably do so. If not, the dental practice must give the patient a readable hard copy, or another format that the patient and dental practice agree to.

However, if the patient asks for an electronic copy of information that the dental practice keeps in an electronic designated record set, the dental practice must be able to provide the information in electronic format. If the dental practice can readily produce the electronic form and format that the patient requested the dental practice must do so. If the dental practice cannot readily produce the electronic form and format that the patient requested, the dental practice must give the information to the patient in the readable electronic form and format that the dental practice and patient agree to. ***A dental practice must be able to produce at least one kind of electronic copy from each of the dental practice's electronic designated record sets*** (Chapter 1, Section 1.E.2).

For example, if a patient asks for an electronic copy of information in an electronic designated record set, and the record set can only produce a hard copy, the dental practice may print the information, scan it, and give the patient an electronic copy of the scanned information.

Summary or Explanation of the information. If the patient agrees in advance, and agrees to any fees that the dental practice would impose, the dental practice may give the patient:

- a summary of the information requested instead of letting the patient see or get copies of the information, or
- an explanation of the information that the individual saw or received a copy of.

Fees. A dental practice may charge only a reasonable, cost-based fee for copies, summaries, and explanations. The fee may include only the cost of:

- labor for copying the information requested (whether in paper or electronic form)
- supplies for creating the paper copies, or for electronic media if the patient asks for a copy on portable media (such as a CD-ROM or USB drive)
- postage, if the patient asked for the copy, summary or explanation to be mailed, and
- preparing a summary or explanation, if the patient agreed to get one (see above)

A dental practice may also choose not to charge for copies.

Denying the Request.
A dental practice must have an appropriate reason ("grounds") to deny a request for access to patient information (see below). HIPAA provides a limited list of permissible grounds for denial. Many of these grounds are complex and highly sensitive (see summaries below). A dental practice should consult qualified legal counsel before denying access.

Under HIPAA some of the permissible grounds for denying access are considered "reviewable." This means that the patient may require the dental practice to provide a review of the denial by a health care professional who did not participate in the original decision to deny access (the "reviewing official"). The dental practice chooses the reviewing official.

HIPAA designates other permissible grounds for denial "unreviewable," which means that the patient does not have a right to a review of the denial.

The reviewable and unreviewable grounds for denial are found in 45 CFR 164.524(a)(2) and (3), respectively. *Some of the grounds for denial have particular requirements that are not discussed below.*

Examples of reviewable grounds for denying a request for access:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- The patient information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

Examples of unreviewable grounds for denying a request for access:

- The patient information requested was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
- The patient information requested consists of certain clinical laboratory information.
- A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of patient information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
- An individual's access to patient information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.
- An individual's access may be denied if the patient information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

To deny a request, the dental practice must give the patient a written denial. The denial must be written in plain language and must contain certain required information. A dental practice should consult qualified legal counsel about the appropriate contents of a written denial of access. If the dental practice has grounds to deny a request to see or get copies of patient information, but the grounds for denial only apply to a part of the requested information, the dental practice must let the patient see or get copies of the portion of the requested information to which the grounds for denial do not apply.

Documentation. A dental practice must document the designated record sets that are subject to access (Chapter 2, Step 4) and the title of the person or office responsible for receiving and processing requests for access (Chapter 2, Step 1). Documentation must be retained for at least six years from the date the document was created, or the date when the document was last in effect, whichever is later (Chapter 2, Step 19).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will provide patients, and their personal representatives as appropriate, access to patient information in a designated record set as required by HIPAA.

Sample Procedures

Staff: If anyone asks to see or get a copy of patient information, politely tell the person that all requests must be in writing and must be reviewed by the Privacy Official. Give the person a copy of our Request for Access form (see *Sample Request for Access*, Appendix 2.14.1) and ask them to fill it out and give it to the Privacy Official.

Privacy Official: *Review requests for access.* Promptly review all completed Request for Access forms (see *Sample Request for Access*, Appendix 2.14.1) to determine whether to the request should be granted or denied in compliance with HIPAA. Access (or written denial of access) must

SAMPLE POLICY AND PROCEDURES

be provided within 30 days of the date that our dental practice received the written request for access, unless our dental practice has properly extended the period for up to 30 additional days.

Verify the identity of the person making the request where appropriate (Chapter 2, Step 6 and *Sample Verification of Identity*, Appendix 2.6).

If our dental practice believes there are permissible grounds to ***deny access***, determine whether the grounds are appropriate and, if so, prepare and send the Denial of Request for Access form. It is prudent to work with qualified legal counsel when denying a request for access. If the grounds for denial are reviewable and the patient or personal representative requests a review, provide an appropriate review of the denial in compliance with HIPAA.

If our dental practice will ***grant a request to see records***, arrange for a time and place in the dental office for the person to see the records within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended). Do not leave anyone unsupervised with original records in any format.

If our dental practice will ***grant a request for copies of records***, provide the copies within the appropriate time frame (within 30 days of the date that the dental practice received the request, or within the extension time period if properly extended).

Fee schedule. If our dental practice will charge for copies, create a schedule of reasonable, cost-based fees for making paper and electronic copies of patient information, for mailing copies in paper and electronic format, and for preparing summaries and explanations of patient information. The fee schedule must comply with both HIPAA and applicable state law.

Electronic copies. ***If a patient requests an electronic copy of a record that our dental practice maintains in an electronic designated record set, our dental practice must provide an electronic copy.*** Our dental practice is not required to provide the exact kind of electronic copy that the patient asks for if we cannot readily do so. If the patient does not agree to the kind of electronic copy that our dental practice can readily produce, offer the patient the information in hard copy.

Do not use outside electronic media in our system if our written risk assessment determined that the risk is unacceptable. Instead, have a supply of blank CD-ROMs and USB drives on hand to use to provide copies of patient information.

A patient has the right to ask for the electronic copy through email (Chapter 1, Section 2.E.2). If the patient prefers an unencrypted email, our dental practice must send the information in an unencrypted email. Our Request for Access Form includes a notice that there is a risk that the information in an unencrypted email could be read by a third party. Use reasonable safeguards to make sure that our dental practice correctly enters the email address.

Sample Forms:

- *Sample Request for Access*, Appendix 2.14.1

Resources:

Office for Civil Rights, *The HIPAA Privacy Rule's Right of Access and Health Information Technology*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf*.

Appendix 2.14.1

Sample Request for Access

This sample form illustrates how a dental practice might document a request for access to patient information.

Privacy Official Name: _____ Telephone: _____

Patient's Name (print): _____

Date of Birth: _____ (for identification purposes)

Describe the records you wish to access and the approximate dates of the records: _____

_____

_____

What would you like for us to do for you?

- ☐ I wish to see the requested records.
- ☐ I wish to get a copy of the requested records.
- ☐ I wish to see and get a copy of the requested records.
- ☐ If the requested records are in an electronic designated record set, I wish an electronic copy of the requested records the following form and format, if readily producible: _____

  _____

  If you would like the information emailed, enter the email address here (PLEASE PRINT VERY CLEARLY!): _____@_____

  We do not recommend sending patient information in an unencrypted email because third parties may be able to access the email.
- ☐ I want you to prepare summary of the requested records and I agree in advance to pay a fee in the amount of $_____.
- ☐ I want you to prepare an explanation of the records that I saw or got a copy of, and I agree in advance to pay a fee in the amount of $_____.
- ☐ I want you to send the copy of the requested records to:

  Name: _____

  Address: _____

Fees

Our practice charges a reasonable, cost-based fee to for copies of patient information, and for postage to mail records if requested.

Questions?
Please contact our privacy official listed at the top of this page if you have any questions about your request to inspect or copy records.

If the request is by a patient:

Patient Signature: _____ Date:_____

If the request is by a patient's personal representative:

Print the Name of the Personal Representative:_____

Relationship to the Patient: _____

I certify that I have the legal authority under federal and state laws to make this request on behalf of the patient identified above.

Signature of Personal Representative:

_____ Date:_____

For Dental Office Use Only

☐ Request for access denied (attach written denial).
☐ Request for access approved.

Step 14.2: Amendment

When a patient asks the dental practice to make a change to his or her patient information.

Note: Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

Where to find the rules:

45 CFR 164.526

What is required:

A dental practice must allow a patient to ask the dental practice to "amend" (insert or append a change to) information about the patient that the dental practice has in a "designated record set" (Chapter 2, Step 4). A dental practice may require the request to be in writing and to provide a reason for the amendment, as long as the dental practice tells patients about these requirements in advance (see *Sample Request for Amendment*, Appendix 2.13.2.1).

Patient records should never be "changed" through erasure, redaction (for example, crossing out), white-out, electronic deletion, etc. Any change to patient records must be made by inserting or appending new information. The original information must remain legible.

A dental practice may refuse to make the amendment if:

- The record or information is not part of a designated record set (Chapter 2, Step 4)
- The information or record is accurate and complete
- The patient does not have the right to see or get a copy of the information (Chapter 2, Step 14.1)
- The dental practice did not create the information or record, unless whoever did create the information or record is no longer available to make the amendment (it is up to the patient to provide a reasonable basis to believe that this is so)

A dental practice has **60 days** to act on a request. If the dental practice cannot act on the request within 60 days of receiving the request, the dental practice may extend the time for up to 30 days by sending the patient, in writing, the reasons for the delay and the date by which the dental practice will complete its action on the request (this must be sent within the original 60-day period) The dental practice may have only one extension. A dental practice must comply with applicable state law that provides a shorter timeframe than HIPAA.

Here is how the dental practice must act on the request:

- **If the dental practice grants the request**, or part of it, then the dental practice must:

  1. Make the amendment by, at a minimum:

     - identifying the records in the designated record set that are affected by the amendment, and
     - "appending" (e.g., adding or attaching) the amendment, or providing a link to the location of the amendment.

2. Tell the patient that the amendment is accepted.
3. Have the patient identify the persons who need to be told about the amendment.
4. Have the patient agree that the dental practice may tell these persons about the amendment.
5. Make a reasonable effort, within a reasonable time, to tell the following persons about the amendment:
    - The persons identified by the patient
    - Other persons (who may include the dental practice's business associates) that the dental practice knows have the information that was amended and that may have relied, or could foreseeably rely, on the information in a way that could harm the patient or cause a problem for the patient

- **If the dental practice denies the request**, or part of it, then the dental practice must provide the patient with a written denial (see *Sample Denial of Request to Amend*, Appendix 2.14.2.2).
    1. If a patient who receives a denial gives the dental practice a "statement of disagreement":
        - the dental practice may write a rebuttal (the patient must be given a copy of the rebuttal)
        - any time the dental practice discloses the patient information that the statement of disagreement relates to, the dental practice must append the following (or an accurate summary):
            - The patient's request for an amendment
            - The dental practice's denial of the request
            - The statement of disagreement (see below), if any
            - The dental practice's rebuttal (see below), if any
    2. If the patient has not given the dental practice a statement of disagreement:
        - any time the dental practice discloses the information that the patient wanted amended, the dental practice must include the following (or an accurate summary), **but only if the patient has asked the dental practice to do so:**
            - The patient's request for an amendment
            - The dental practice's denial of the request

Standard Transactions: If the dental practice is making an electronic standard transaction that does not permit the additional material to be included, the dental practice may transmit the material separately.

Documentation: A dental practice must document the titles of the persons or offices responsible for receiving and processing requests for amendments (Chapter 2, Step 1).

SAMPLE POLICY AND PROCEDURES

Sample Policy

A patient, and a personal representative as appropriate, has the right to ask our dental practice to amend information about the patient in a designated record set if they believe that the information is not correct. As stated in our Notice of Privacy Practices, the request must be in writing and must give the reason for the amendment. If we deny the request, we will put our reason for denying the request in writing. If we agree to make the amendment, we will amend the record and tell the patient. If another HIPAA covered entity (such as a dental plan or a specialist) tells our practice that they made amendment to information about a patient, we will make the amendment to information in our designated record set, as appropriate.

Sample Procedures

Staff: If a patient (or patient's personal representative) asks to amend any information in our dental practice's records, politely tell them that the request must be in writing and give them a copy of the Request for Amendment form (see *Sample Request for Amendment*, Appendix 2.14.2.1). Ask the patient to complete the form and give it to the Privacy Official. Only the Privacy Official may receive and process requests for amendments. Immediately report a request to the Privacy Official.

Privacy Official: You are responsible for receiving and processing all requests to amend patient records.

Requests to amend patient records must be made in writing using our Request for Amendment form (see *Sample Request for Amendment*, Appendix 2.14.2.1). The request must include a reason for the amendment. Make sure our Notice of Privacy Practices states that requests to amend records must be in writing and must state the reason for the request.

Act on all requests within 60 days [or shorter state law timeframe] of the date that our dental practice receives the request. If our dental practice requires more than 60 days to act on a request for amendment, then, within the 60-day period, extend the time period for up to 30 days by providing the patient with a letter stating the reasons for the delay and the date by which our dental practice will complete its action on the request. We may only have one extension.

Review each requested amendment, and determine whether the request should be approved or denied.

If our dental practice approves the amendment, append the amendment to the record, tell the patient that the amendment is approved, ask the patient who needs to be told about the amendment, ask the patient to agree that the dental practice may tell these persons about the amendment, and make a reasonable effort to send notice of the amendment within a reasonable time to the persons identified by the patient and to any other persons that we know have the information that we amended and may have relied on it (or may rely on it in the future) in a way that could harm the patient or put the patient at a disadvantage.

If our dental practice denies the amendment, send a written denial to the patient that contains the information required by HIPAA (see *Sample Denial of Request to Amend*, Appendix 2.14.2.1). If the patient gives us a statement of denial, determine whether our dental practice should write a rebuttal (and, if so, draft and provide the rebuttal).

SAMPLE POLICY AND PROCEDURES

Future disclosures of the information:
*If the patient gives us a statement of denia*l, ensure that every time our dental practice discloses the information in question, we include the request for amendment, our denial, the statement of disagreement, and our rebuttal (if any), or an accurate summary of these documents.

If the patient does not give us a statement of denial, but the patient asks our dental practice to include the request for amendment and our denial whenever our dental practice discloses the information in question, ensure that copies of these documents (or an accurate summary) is included in all such disclosures.

If the dental practice is making an electronic standard transaction that does not permit the additional material to be included, transmit the material separately.

Documentation: Document all requests for amendment, and log all requests for amendment and their disposition (see *Sample Amendment Request Log*, Appendix 2.14.2.3), and retain the documentation for at least six years from the date of its creation, or from the date last in effect, whichever is later (Chapter 2, Step 19).

Sample Forms:

- *Sample Request for Amendment*, Appendix 2.14.2.1
- *Sample Denial of Request to Amend*, Appendix 2.14.2.2
- *Sample Amendment Request Log*, Appendix 2.14.2.3

Appendix 2.14.2.1
Sample Request for Amendment

This sample form illustrates how a dental practice might document a patient's request to amend the patient's protected health information in the practice's designated record set.

To the Patient: Please use this form to ask our dental practice to change any information about you in our records. All requests for changes to our records must be in writing and must state the reason for the change. You must return this form to the Privacy Official listed on the bottom of this form.

Patient Information

Name of Patient (print name): _____

Patient's Date of Birth: _____ Today's Date: _____

Patient Signature: _____ Date: _____

For Personal Representative of the Patient:

Your Name: _____

Your Relationship to Patient: _____

Personal Representative Signature: _____ Date: _____

I hereby certify that I have legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____ Date: _____

Requested Amendment

Please describe in detail how you want your records changed: _____

_____

_____

Reason for requested change: _____

_____

Contact Person

Please contact the dental practice's Privacy Official if you have any questions relating to your request to amend records.

Privacy Official Name: _____

Address: _____

Telephone Number: _____

Appendix 2.14.2.2
Sample Denial of Request to Amend

This sample form illustrates how a dental practice might notify a patient that the dental practice has denied the patient's request to amend information in a designated record set.

Patient's Name: _____

Patient's Address: _____

Name of person who requested the change: _____

Dear _____ ,

We are responding to your request to amend patient information. We have reviewed the request carefully and we have determined that we cannot approve the amendment that you asked for.

This is the reason for that we cannot approve the amendment:

- ☐ The information or record is not in a designated record set
- ☐ The information or record is accurate and complete
- ☐ The patient does not have a right to access the information or record
- ☐ The dental practice did not create the information or record

You have the right to give us a written statement disagreeing with this denial. The statement may not be longer than one page. If you would like to give us a statement, please mail it to our Privacy Official at the address below. If you do not give us a statement of disagreement, you may ask us to give your request for amendment and our denial every time we disclose the information that you wanted us to amend.

If you are concerned that we may have violated your privacy rights, or you disagree with a decision we made about your health information or in response to a request you made, you may file a complaint with our dental office using by contacting our Privacy Official at the address below, or calling our Privacy Official at **<telephone number>**. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request, or you can follow the instructions at on this web page: *http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html*.

If you have any questions about this notice, please contact:

Privacy Official: _____

Address: _____

Telephone Number: _____

Appendix 2.14.2.3

Sample Amendment Request Log

This sample form illustrates how a dental practice might document the practice's responses to patient requests to amend information in a designated record set.

Patient Name	Amendment Requested	Approved or Denied?	If Approved:		
			Date Amendment Completed	List any Third Parties who must be notified of the amendment	Date Amendments Sent to Third Parties

Step 14.3: Accounting of Disclosures

When a patient asks for a list of the dental practice's disclosures of the patient's information.

Note: Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

Where to find the rules:

45 CFR 164.528

What is required:

A patient has the right to an accounting of disclosures of the patient's information that the dental practice made in the six years prior to the date of the request.

When a patient asks for an accounting of disclosures, the dental practice has **60 days** to provide the accounting requested. If the dental practice cannot provide the accounting in 60 days, it may extend the time by up to 30 days by giving the patient a written statement of the reasons for the delay and the date by which the dental practice will provide the accounting. A dental practice must send the patient the written statement during the original 60-day period. A dental practice may have only one 30-day extension.

A patient is entitled to one free accounting of disclosures in any 12-month period. If a patient asks for one or more additional accountings of disclosures in any 12-month period, the dental practice may provide the additional accounting(s) for free, or may charge the patient a reasonable, cost-based fee, as long as the dental practice tells the patient about the fee in advance and gives the patient the chance to withdraw or change the request in order to avoid or reduce the fee.

The dental practice must document the following, and retain each document for at least six years from the date the document was created, or the date the document was last in effect, whichever is later:

- For each disclosure that would need to be in an accounting of disclosures, the dental practice must log the disclosure and all of the information that would have to be included in the accounting (see below, and see *Sample Log of Disclosures of Patient Information*, Appendix 2.14.3.1)
- A copy of any accounting of disclosures that the dental office provides
- The titles of the person(s) or office(s) responsible for receiving and processing requests for an accounting of disclosures (Chapter 2, Step 1)

Providing an accounting of disclosures

Certain kinds of disclosures of patient information do **not** need to be included in the accounting. For example, the accounting is ***not*** required to include:

- Disclosures for treatment (such as appropriate disclosures of patient information to a specialist who will treat the patient)
- Disclosures for payment (such as appropriate disclosures of patient information to a dental plan for payment purposes)
- Disclosures for health care operations (such as disclosures for appropriate purposes related to business management of the dental practice)
- Disclosures to patients of their own information

- "Incidental" disclosures (Chapter 2, Step 20)
- Disclosures that the patient authorized by signing an authorization form (Chapter 2, Step 9)
- Disclosures to persons involved in the patient's care or payment for care of information relevant to their involvement or information about the patient's location, general condition or death, if:
    - o the patient is present or available and agrees, the patient has the opportunity to object and does not object,
    - o the dental practice exercises professional judgment to infer that the patient does not object to the disclosure, or if
    - o the patient is not present, or the patient is incapacitated or there is an emergency, and the dental practice exercise professional judgment and determine the disclosure is in the patient's best interest
- If the dental practice provides medical supplies, x-rays, or similar forms of patient information to someone involved in the patient's care, relying on professional judgment and experience with common practices and in the best interest of the patient
- Uses and disclosures to a disaster relief organization to help provide information to someone involved in the patient's care as discussed above
- If the patient is deceased, uses and disclosures to persons involved in the patient's care or payment for care, if the information is relevant to the person's involvement and the patient had not expressed a preference against the disclosure
- Certain disclosures for national security or intelligence purposes (see 45 CFR 164.512(k)(2))
- Certain disclosures to correctional institutions or law enforcement (see 45 CFR 164.512(d)(5))
- Certain disclosures as part of a limited data set for certain research, public health, or health care operations (Chapter 2, Step 21), or
- Disclosures that were made before the dental practice was required to comply with HIPAA

Law enforcement and health oversight. In certain situations, a dental practice must temporarily suspend an individual's right to receive an accounting of the disclosures that the dental practice makes to a law enforcement official or a health oversight agency if providing an accounting would impede the activities of the official or agency. If an official or agency tells the dental practice not to tell the patient that the dental practice disclosed the patient's information to the official or agency, the dental practice must comply with the requirements in 45 CFR 154.528(a)(2).

Contents of the Accounting of Disclosures

Except for the kinds of disclosures that do not need to be included in the accounting (see above), the accounting must include all disclosures of the patient's "protected health information" (see Chapter 3) made by the dental practice that occurred during the six years prior to the request, unless the patient requests an accounting for a shorter period of time.

For each disclosure, the accounting must include:

1. The date of the disclosure
2. The name of the entity or person who received the information, and, if known, their address

3. A brief description of the information disclosed
4. A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis of the disclosure[17]
5. If the dental practice made multiple disclosures to a single person or entity for the same purpose, the dental practice might be able to group them on the accounting. See 45 CFR 164.528(b)(3).
6. Special rules apply to listing disclosures for research purposes. See 45 CFR 164.528(b)(4).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Upon request, our dental practice will provide a patient with an appropriate accounting of disclosures.

Sample Procedures

Staff: Every patient has the right to ask our dental practice for an "accounting of disclosures" of the patient's information.

Immediately report to the Privacy Official any disclosures of patient information that are not for purposes of treatment, payment, or healthcare operations. Tell the Privacy Official the date of the disclosure, who received the patient information, the information that was disclosed, and the purpose of the disclosure.

The Privacy Official is responsible for receiving and processing all requests for an accounting of disclosures. If a patient asks you for an accounting of disclosures, politely tell them that our Privacy Official handles these requests, give them a copy of our request form, and ask them to complete the form and to give it to the Privacy Official.

Privacy Official: Use the Log of Disclosures of Patient Information (see *Sample Log of Disclosures of Patient Information*, Appendix 2.14.3.1) to record all disclosures of patient information that would need to be included if a patient asks for an accounting of disclosures. Since an accounting of disclosures must include disclosures made up to six years before the request, make sure information about each of disclosure in the log is retained for at least six years from the date of the disclosure.

If a patient asks for an accounting of disclosures, have the patient complete the Patient Request for Accounting of Disclosures form (see *Sample Request for Accounting of Disclosures*, Appendix 2.14.3.2).

Within **60 days** of the date that our dental practice receives the request:

- provide the accounting of disclosures, or
- if our dental practice cannot provide the accounting within the 60-day period, send the patient a letter extending the period for up to 30 days. The letter must state the reasons for the delay and the date on which we will provide the accounting. We are only entitled to one 30-day extension. Provide the accounting to the patient at the end of the extension period.

SAMPLE POLICY AND PROCEDURES

Maintain documentation of every request for an accounting of disclosures, every accounting of disclosures that our dental practice provides, and your designation as the person responsible for receiving and processing requests for accountings of disclosures (Chapter 2, Step 1) for at least six years from the date of the document's creation or the date when the document was last in effect, whichever is later (Chapter 2, Step 19).

Every patient is entitled to one free accounting of disclosures in any 12-month period. Determine whether our dental practice will charge a fee for requesting additional accountings of disclosures in a 12-month period, or whether all accountings of disclosure will be provided for free. If a fee will be charged, determine the permissible, reasonable cost-based fee for providing an accounting of disclosures. If a patient or personal representative requests an additional accounting of disclosures within a 12-month period, inform them of the fee and permit them to cancel or change the request in order to avoid or reduce the fee.

Sample Forms:

- *Sample Log of Disclosures of Patient Information*, Appendix 2.14.3.1
- *Sample Request for Accounting of Disclosures*, Appendix 2.14.3.2

[17] A copy of a written request for disclosure can be used instead of the brief statement, if the disclosure was to HHS in connection with a HIPAA investigation, or if the disclosure was a permitted disclosure that HIPAA permits the dental practice to make without having the patient sign an authorization form, or giving the patient the opportunity to agree or object (Chapter 2, Step 8).

Appendix 2.14.3.1

Sample Log of Disclosures of Patient Information

This sample form illustrates how a dental practice might log disclosures of patient information, so that the practice is prepared in case a patient asks for an accounting of disclosures.

Patient Name	Date of Disclosure	Who received the information?	Description of protected health information disclosed	Purpose of Disclosure	Was the disclosure for research?	Is this one of multiple disclosures that can be grouped?

Appendix 2.14.3.2

Sample Request for Accounting of Disclosures

This sample form illustrates how a dental practice might document a patient's request for an accounting of disclosures of the patient's protected health information.

Notice to Patients: Please use this form to make a request that our practice provide you with an accounting of disclosures of your protected health information.

Patient Name: _____

Disclosure Accounting Request

Time Frame

Please specify the dates between which you would like for our practice to account for disclosures of your protected health information. Under HIPAA, we are not required to include certain disclosures, including disclosures for treatment, payment or healthcare operations.

Starting Date for Disclosure: _____

Ending Date for Disclosure: _____

Our Practice's Contact Person

Please contact _____, our practice's Privacy Official if you have any questions relating to your Accounting of Disclosures request.

Patient Information

Print Name: _____

Signature: _____ Date: _____

Patient's Date of Birth: _____

Step 14.4: Confidential Communications

When a patient asks the dental practice to contact him or her in a different way or at a different place.

Note: Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

Where to find the rules:

45 CFR 164.522 (b)

What is Required:

A dental practice must allow patients to ask to the dental practice to send them communications in a different way or at a different location. A dental practice must agree to the request if it is reasonable. For example, a patient may ask the dental practice to contact the patient by mail rather than leaving a voice message, or to contact the patient at a different address or a different phone number.

A dental practice may require requests for confidential communications to be in writing, and require the patient to specify the alternative address or other method of contact. When appropriate, a dental practice may require a patient to provide information about how any payments will be handled before the dental practice agrees to a request for confidential communications.

A dental practice may not require the patient to explain why he or she is asking for confidential communications.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our practice will accommodate reasonable requests by patients to receive communications from our practice by an alternative means or at an alternative location.

Sample Procedures

Staff: If a patient asks our dental practice to contact him or her in a different way or at a different location, ask the patient to fill out our Confidential Communications form (see *Sample Request for Confidential Communications*, Appendix 2.14.4). Do not ask the patient to explain why he or she is making the request.

When our practice has agreed to a request for confidential communications, flag the patient's record. If you are communicating with a patient whose record is flagged, make sure to abide by the confidential communications request.

Privacy Official: Develop a Confidential Communications form (see *Sample Request for Confidential Communications*, Appendix 2.14.4) for our dental practice and train staff to use the form when appropriate.

Develop a system to flag patient records to ensure that our dental practice abides by any requests for confidential communications that we agree to. *The flag should not indicate to anyone other than our workforce that the patient has requested confidential communications. For example, use a color-coding system or other neutral indicator if paper files are flagged. This will help protect patient confidentiality and prevent unauthorized people from knowing about the request.*

SAMPLE POLICY AND PROCEDURES

Retain the completed forms for at least six years from the date they were completed, or the date when they were last in effect, whichever is later (Chapter 2, Step 19).

Sample Forms:

- *Sample Request for Confidential Communications*, Appendix 2.14.4

Appendix 2.14.4

Sample Request for Confidential Communications

This sample form illustrates how a dental practice might document a patient's request that the practice communicate with the patient in a different way or at a different place.

To the Patient: Use this form if you would like our dental practice to communicate with you other than at your primary phone number and/or address. Fill out this request in its entirety.

Patient Name (print): _____

Alternative Communication Request (Please tell us the way you would like us to communicate with you, and/or the address you would like us to use): _____

_____

_____

Payment Information
Your request may affect our normal billing and payment procedure. Please specify any alternative method for handling payment.

_____

_____

Caution: there is some level of risk that third parties might be able to read unencrypted emails.

Patient Signature: _____ Date: _____

For Personal Representatives of the Patient

Print Name of Personal Representative:_____

Relationship to the Patient: _____

Step 14.5: Restricted Disclosure

When a patient asks the dental practice not to disclose his or her information.

Note: Although we refer to the "patient" in this section, keep in mind that in appropriate circumstances a patient's personal representative may exercise these rights on behalf of the patient.

Where to find the rules:

45 CFR 164.522(a)

The 2013 Final Rule changed the requirements for restricted disclosures. See Chapter 1, Section 2.D. for a discussion of the changes.

What is Required:

A dental practice must allow a patient to ask the dental practice not to use or disclose information about the patient. In general, a dental practice is not required to agree to a restriction. However, an exception was created by the 2013 Final Rule. As of September 23, 2013, a dental practice must agree if a patient asks the dental practice not to disclose information to a health plan as long as:

- the information was for the purpose of carrying out payment or health care operations and is not otherwise required by law, *and*
- the information pertained 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.

For example, if a dental practice is paid in full by the patient (or by someone on behalf of the patient, such as a family member or even a different plan), and the patient asks the dental practice not to disclose information about the service to a health plan for payment or health care operations purposes, the dental practice must agree to the restriction and abide by it. The dental practice may not submit a claim to the health plan for the service, permit the health plan to review or audit information about that service, or otherwise disclose information about the service to the health plan.

Other than the health plan restriction discussed above, a dental practice is not required to agree to a request to restrict use or disclosure. However, if a dental practice does agree, it must abide by the restriction until the restriction is terminated (see below).

Exceptions to restrictions. Even if a dental practice agrees to a requested restriction, the dental practice may use or disclose the restricted information in the following situations:

1. *Emergency Treatment:* If the patient needs emergency treatment, and the restricted information is needed for such treatment, the dental practice may use the restricted information to provide the emergency treatment. The dental practice may also disclose the restricted information to a health care provider to provide the emergency treatment, but the dental practice must ask the health care provider not further use or disclose the information.

2. *HHS Investigation:* A dental practice must disclose patient information, whether or not it is restricted, if HHS asks for the information in connection with an investigation to determine HIPAA compliance.

3. *Permitted Uses and Disclosures:* An agreement to restrict disclosure is not effective to prevent uses or disclosures for which an authorization or opportunity to agree or object is not required (Chapter 2, Step 8.14). This category of permitted uses and disclosures generally involves certain public health activities, disclosures to FDA about products, victims of abuse, neglect or domestic violence, health oversight activities, judicial proceedings, law enforcement purposes, decedents, research, averting a serious threat to health or safety, government functions, and workers' compensation.

Terminating a restriction.
Termination by the patient. Patients can cancel (or agree to cancel) a restriction at any time but the cancelation must be documented. If the patient cancels the restriction in writing, then the writing is the documentation. If the patient cancels the restriction orally, then the dental practice must document the cancelation.

Termination by the dental practice. A dental practice can cancel a restriction, except for the health plan restriction discussed above, by telling the patient that the dental practice is canceling its agreement to restrict the information. However, the cancelation does not apply to information about the patient that the dental practice created or received before the dental practice told the patient about the cancelation.

Documentation. HIPAA requires a dental practice to document all restrictions that the dental practice agrees to and retain the documentation for at least six years from the date the documentation was created, or from the date when the documentation was last in effect, whichever is later (Chapter 2, Step 19). A dental practice is not required to document requests for restrictions that it does not agree to (however, keep in mind that a dental practice is required to agree to an appropriate request for nondisclosure to a health plan, as discussed above).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our practice allows patients to request restricted use or disclosure of their patient information As of September 23, 2013, HIPAA requires our dental practice to agree to a request not to disclose information to a health plan about a health care item or service for payment and health care operations purposes when our dental practice has been paid for in full for the item or service by the patient or by a third party, unless the disclosure is required by law. Our dental practice is not required to agree to any other kind of request for restriction, but if we do we must abide by the restriction until it is terminated.

Sample Procedures

Staff: If a patient asks you not to use or disclose his or her information in a certain way, politely tell them that only our Privacy Official can respond to requests for restrictions and ask them to contact our Privacy Official.

Privacy Official: You are responsible for responding to all requests to restrict the use or disclosure of patient information. Determine whether our dental practice will require requests for restrictions to be in writing and, if so, develop an appropriate request form (see *Sample Request for Restricted Use or Disclosure*, Appendix 2.14.5). Whether or not our dental practice requires requests to be in writing, document all requests for restrictions that our dental practice agrees to. Retain all completed documentation for at least six years from the date the document was completed, or at least six years from the date that the document was last in effect, whichever is later (Chapter 2, Step 19).

Health Plan Restriction. As of September 23, 2013, our practice will agree to any request not to disclose patient information about a health care item or service to a health plan (medical or dental) for purposes of carrying out payment or health care operations if the information pertains solely to a health care item or service for which our dental practice has been paid in full, unless otherwise required by law. This applies whether the patient pays in full or if payment comes from another source (including another plan).

SAMPLE POLICY AND PROCEDURES

Write up any necessary procedures to comply with this provision, put them into action and train staff to comply. For example, our dental practice must flag restricted information so a claim is not submitted to the health plan, and the health plan does not review the information during an audit.

Other restrictions. Except for the health plan restriction discussed above, our dental practice is not required to agree to a requested restriction. Generally, our dental practice will agree to restrictions only in exceptional circumstances, and when our dental practice can reasonably accommodate them. Determine whether or not we should agree to each request.

If we agree to a restriction, we must not violate the restriction; however, we may use and disclose restricted information in certain situations, such as emergency treatment, HHS investigation, and public health reporting as permitted by HIPAA.

If we agree to a restriction, the agreement can only be terminated in three ways:

1. The patient requests the termination in writing.
2. The patient orally agrees to the termination and our dental practice documents the oral agreement.
3. Our dental practice informs the patient that we are terminating our agreement to a restriction (However, our dental practice cannot terminate health plan restrictions where our dental practice has been paid in full – see above). The termination only applies to patient information that our dental practice created or received *after* we informed the patient that the restriction has been terminated.

Sample Forms:

- *Sample Request for Restricted Use or Disclosure*, Appendix 2.14.5

Appendix 2.14.5

Sample Request for Restricted Use or Disclosure

This sample form illustrates how a dental practice might document a patient's request for a restriction on the use or disclosure of the patient's information.

Please check and complete either A or B, as applicable.

☐ **A. Health Plan Restriction for items/services paid for in full.**

Patient Name: _____ (please print) asks the dental practice not to give information about the following item(s) and/or service(s), for which the dental practice has been paid in full, to the health plan indicated below, for purposes of payment or health care operations, unless required by law:

Item(s) or service(s): _____

Health plan: _____

*I understand that the dental practice **must agree** to this requested restriction if the practice has received payment in full for these item(s) or service(s).*

Patient Signature: _____ Date: _____

Dental Practice: has payment in full been received? ☐

Dentist or Administrator's Signature:

_____ Date: _____

☐ **B. Other Restriction.**

Patient Name: _____ (please print) asks the dental practice not to use or disclose the information indicated below in the manner indicated below:

Description of information: _____

_____

Requested restricted use and/or disclosure: _____

_____

*I understand that the dental practice **is not required** to agree to this requested restriction, but that if the dental practice does agree it can end the restriction by telling me. I understand that if the dental practice agrees to the restriction, the dental practice may use and disclose the restricted information in certain circumstances, such as for emergency treatment or public health disclosures.*

Patient Signature: _____ Date: _____

Dentist or Administrator's Signature:

_____ Date: _____

For Dental Office Use Only

☐ Agree to

☐ Not Agree to

NOTE: The dental practice **must agree** to a request for disclosure to a health plan of information about a health care item or service for which the dental practice has been paid in full (see Section A of this form).

Signature: _____ Date: _____

Step 15: Training

HIPAA requires a dental practice to train workforce members to comply with the dental office's HIPAA policies and procedures.

Where to find the rules:

45 CFR 164.530(b);

What is required:

A dental practice must train all of its "workforce members," including management, on the HIPAA privacy, security and breach notification policies and procedures that they need to know about to do their jobs.

A "workforce member" is a dental practice's employee, volunteer, trainee, or anyone else:

- who works for the dental practice, and
- whose work is under the direct control of the dental practice, whether or not the person is paid by the dental practice.

HIPAA requires a dental practice to train new workforce members within a reasonable period of time after they join the dental practice. However, to protect patient confidentiality and protect the practice from liability for HIPAA violations, it would be prudent to provide training before a new workforce member is permitted access to patient information.

When there is a material change in dental practice's privacy or breach notification policies and procedures, the dental practice must provide training updates within a reasonable period of time after the change becomes effective to all workforce members whose jobs are affected by the change.

All training must be documented (see *Sample HIPAA Training Sign-in Sheet*, Appendix 2.15). Training documentation must be retained at least six years from the date the document was created, or six years from the date when it was last in effect, whichever is later. (Chapter 2, Step 19).

Chapter 7, *Training is the Key to Compliance*, includes a discussion of HIPAA training and sample training topics.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will train all workforce members within a reasonable period of time after they join the practice to comply with the HIPAA policies and procedures that affect their jobs. When there is a material change to our policies and procedures, our dental practice will train the workforce members whose jobs are affected by the change within a reasonable time after the change becomes effective.

Sample Procedures

Staff: You must be trained to comply with HIPAA when you do your job. All training must be documented. When there is a material change to our HIPAA policies and procedures that affect your job, you will receive a training update.

SAMPLE POLICY AND PROCEDURES

Privacy Official: You are responsible for making sure that each of our workforce members get the HIPAA training they need to do their jobs, including training updates when there is a material change in our HIPAA policies and procedures. You must make sure that new workforce members get HIPAA training within a reasonable time after joining the dental practice. When we change our policies and procedures, make sure that the workforce members affected by the change get training within a reasonable time after we put the change into effect.

You must document all HIPAA training, even on-the-spot refreshers. Keep the training documentation for at least six years from the date the document was created or from the date when the document was last in effect, whichever is later.

In some cases, retraining may be an appropriate sanction for a workforce member who violates one of our HIPAA policies or procedures (Chapter 2, Step 16). When retraining is used as a sanction, make sure a copy of the training documentation is placed in the person's personnel file.

Sample Forms:

- *Sample HIPAA Training Sign-in Sheet*, Appendix 2.15

Appendix 2.15

Sample HIPAA Training Sign-in Sheet

This sample form illustrates how a dental practice might document that the dental practice's workforce members have received HIPAA training.

Name of Trainer: _____

Trainer's Company Affiliation: _____

Length of Training: _____ Date of Training: _____

Topics Included in Training (attach outline): _____

_____

_____

_____

_____

_____

Attendee List

Print Name	Signature	Date

Step 16: Disciplinary Action ("Sanctions")

Where to find the rules:

45 CFR 164.530(e)

What is required:

"Sanctions" refers to disciplinary action. A dental practice must have appropriate sanctions for workforce members who do not comply with the dental practice's HIPAA privacy, security and breach notification policies and procedures, and apply the sanctions when appropriate. Sanctions must be documented and the documentation must be retained for at least six years from the date the document was created or from the date when the document was last in effect, whichever is later (Chapter 2, Step 19).

Examples of sanctions that may be appropriate, depending on the circumstances, include verbal and written warnings, retraining, suspension, and termination.

Whistleblowers (Chapter 2, Step 8). A dental practice may not apply sanctions against a whistleblower who makes a permitted use or disclosure of patient information.

Intimidation and retaliation (Chapter 2, Step 17). A dental practice may not use sanctions as a means of intimidating or retaliation against a workforce member who:

- files a HIPAA complaint with the government,
- cooperates with a government HIPAA investigation or proceeding, or
- opposes any activity at the dental office that the workforce member believes is unlawful under HIPAA, as long as
  - the workforce member's belief is reasonable and in good faith, and
  - the workforce member opposes the activity in a reasonable way and does not impermissibly use or disclose patient information.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will have and apply appropriate sanctions against workforce members who violate our HIPAA privacy, security and breach notification privacy policies and procedures. Our dental practice will document all sanctions that are applied.

Sample Procedures

Staff: Our dental practice applies appropriate sanctions against workforce members who violate our HIPAA privacy, security and breach notification policies and procedures.

Privacy Official: If you discover that a workforce member has violated our HIPAA policies and procedures, you must apply an appropriate sanction.

Every time a sanction is applied, you will document the sanction and retain the documentation for six years from the date the document was created or from the date when the document was last in effect, whichever is later.

Sanctions must not be imposed against whistleblowers whose actions are appropriate under the HIPAA Privacy Rule. Sanctions must not be used as a means of retaliation or intimidation in violation of HIPAA.

Step 17: Retaliation and Intimidation

A dental practice and its business associates are prohibited from intimidating or retaliating against a person who exercises his or her rights under HIPAA.

Where to find the rules:

45 CFR 164.530(g)
45 CFR 160.316

What is required:

A dental practice or its business associate may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against a person because he or she:

- exercises any right established under the Privacy Rule or Breach Notification Rule
- participates in any process provided for by the Privacy Rule or Breach Notification Rule
- files a complaint with the dental practice or with the government concerning the dental practice or business associate's HIPAA compliance
- testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing
- opposes any act that HIPAA makes unlawful, as long as the person has a good faith belief that the act is unlawful, and the way the person opposes the act is reasonable and does not involve disclosing patient information in violation of HIPAA

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will not intimidate or retaliate against anyone who exercises their rights under HIPAA, participates in a HIPAA process, files a HIPAA complaint, participates in a HIPAA investigation, compliance review, proceeding or hearing (e.g., by testifying or assisting), or who appropriately opposes an act that they believe is unlawful under HIPAA. Neither will our dental practice permit our business associates to do so.

Sample Procedures

Staff: Our dental practice will not, and will not permit our business associates to, intimidate, threaten, coerce, or discriminate against any person, nor take any other retaliatory action against anyone, because he or she:

- exercises a HIPAA right
- participates in a process provided for by the Privacy Rule or Breach Notification Rule
- files a complaint with the dental practice or with the Secretary of HHS concerning the HIPAA compliance of the dental practice or a business associate
- testifies, assists, or participates in a HIPAA investigation, compliance review, proceeding, or hearing by HHS

SAMPLE POLICY AND PROCEDURES

- opposes any act or practice that HIPAA makes unlawful, as long as the person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of patient information in violation of the Privacy Rule

Immediately report to the Privacy Official if you believe or suspect that anyone at our dental practice, or at one of our business associates, has intimidated or retaliated against you or anyone else.

Privacy Official. If you discover that anyone at our dental practice or at one of our business associates has intimidated or retaliated against someone in violation of this policy, ensure that the intimidation or retaliation stops. See that appropriate sanctions are applied against any workforce member responsible for the intimidation or retaliation, and document the sanctions. If a business associate engages in impermissible intimidation or retaliation in violation of HIPAA, take reasonable steps to end the violation by the business associate. If the attempt to end the violation is not successful, the dental practice must terminate the business associate agreement, if feasible.

Step 18: Waiver of HIPAA Rights

Your dental practice may not require anyone to waive a HIPAA right in order to get treatment, or for payment, enrollment in a health plan, or eligibility for benefits.

Where to find the rules:

45 CFR 164.530(h)
45 CFR 160.306

What is required:

A dental practice may not require a patient or anyone else to waive any of the following rights as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits:

- their right to complain to the Secretary of HHS if they believe that the dental practice or another HIPAA covered entity is not complying with HIPAA, or
- any other rights that they have under the Privacy Rule or the Breach Notification Rule.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will not require anyone to waive their right to complain to HHS if they believe our dental practice or another HIPAA covered entity is not complying with HIPAA, or any other rights that they have under the Privacy or Breach Notification Rule, as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Sample Procedures

Staff: Do not ask patients to waive a HIPAA right as a condition of treatment, payment, health plan enrollment or eligibility for benefits.

Privacy Official: Train all workforce members to understand that they may not require or request a patient or other person to waive:

- any right under the Privacy Rule or Breach Notification Rule, or
- their right to file a HIPAA complaint with HHS

as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Step 19: Documentation of HIPAA Compliance

A dental practice must maintain documentation as required by HIPAA.

Where to find the rules:

45 CFR 164.530(j)
45 CFR 160.310

What is required:

HIPAA requires a dental practice to develop and collect a wide range of documents. For example, a dental practice must develop written policies and procedures and a Notice of Privacy Practices, document the designation of the Privacy Official, enter into business associate agreements, and document training and any sanctions applied against workforce members who fail to comply with the dental practice's HIPAA policies and procedures.

A dental practice must maintain this documentation in paper or electronic form. It may be more convenient to manage and retain the documentation electronically, but dental practices that maintain their HIPAA compliance documentation electronically should make certain they have current backups so that the documentation is always accessible. For example, if a dental practice is selected for a HIPAA audit, the practice may have as little as 10 days to produce copies of its compliance documents.

A dental practice must not dispose of any HIPAA compliance document for at least six years after it was created, or six years when it last was in effect, whichever is later. Some HIPAA documents must be retained for a very long time

This HIPAA requirement does not apply to the retention of patient information, such as dental records and billing records, which is generally governed by state law, unless a HIPAA documentation requirement also applies.

A dental practice should keep its HIPAA compliance documentation readily accessible because the federal government can require a dental practice to produce the documentation on very short notice — for example, if the federal government investigates whether the dental practice is complying with HIPAA.

Staff should be trained to appropriately retain the documentation, and not to dispose of it until the proper time. A single untrained staff member cleaning out a filing cabinet could make it very difficult for a dental practice to demonstrate to the federal government that the dental practice has complied with HIPAA, which could result in penalties.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will maintain the following documentation as required by HIPAA:

- HIPAA privacy and breach notification policies and procedures
- Communications required by to be in writing
- Documentation of actions, activities, and designations required to be documented

Our dental practice will retain this documentation for a period of at least at least six years after its creation or last effective date, whichever is later.

SAMPLE POLICY AND PROCEDURES

Sample Procedures

Staff: Do not dispose of, delete or destroy any electronic or paper HIPAA document for six years from the date the document was created, or six years after it was last in effect, whichever is later. Examples of HIPAA documents include policies and procedures, Notices of Privacy Practices, acknowledgment forms, authorization forms, breach notification documents, etc.

Privacy Official: Maintain an electronic and/or hard copy file of our HIPAA compliance documentation.

Our HIPAA compliance documentation includes a variety of documents. Here are some examples of HIPAA compliance documentation:

- current and past designation of Privacy Official
- policies and procedures
- Notices of Privacy Practices
- business associate agreements
- signed acknowledgments of receipt of Notice of Privacy Practices
- training sign-in sheets
- signed authorization forms
- complaints about our privacy practices
- documentation of disciplinary actions ("sanctions")
- restricted disclosures
- disclosure logs
- lists of designated record sets
- minimum necessary restrictions
- breach notification letters
- logs of breaches involving fewer than 500 patients

Our HIPAA documentation must contain current versions of documents such as policies and procedures, Notice of Privacy Practices, and personnel designations. Our HIPAA documentation must also contain any prior versions of those documents unless at least six years has passed since the document was created or since the document was last in effect, whichever is later. Ensure that all required HIPAA documentation is not disposed of, deleted, destroyed, or lost for at least at least six years from the date of its creation or the date when last in effect, whichever is later.

Dispose of HIPAA compliance documentation when it is appropriate to do so. If a document identifies or could be used to identify a patient, dispose of the document in a way that "secures" the document under the Breach Notification Rule (Chapter 2, Step 22). Hard copy documents should be shredded or destroyed such that the patient information cannot be read or otherwise reconstructed. Electronic media containing patient information should be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, such that the patient information cannot be retrieved.

Step 20: Safeguard Patient Information

Have in place appropriate safeguards to protect the privacy of all forms of patient information.

Where to find the rules:

45 CFR 164.530(c)

What is required:

Patient information can be in a variety of forms, such as paper, films, photographs, spoken information, and electronic information such as electronic dental records. A dental practice must have safeguards in place to protect patient information in all forms.

There are three categories of safeguards: administrative, technical, and physical.

- Administrative safeguards concern what workforce members do and how security measures are chosen and put into action.
- Technical safeguards involve the technology used for patient information and the policies and procedures for using and accessing that technology.
- Physical safeguards protect patient information, the places and equipment where patient information is located, and the building itself from unauthorized intrusion.

A dental practice must have all three categories of safeguards in place and must reasonably safeguard patient information in all forms from both deliberate and accidental uses or disclosures that violate the Privacy Rule.

The dental practice's Security Official is responsible for developing safeguards for electronic patient information and putting them into action (see Chapters 4, 5, and 6). The Privacy Official must develop safeguards that comply with the Privacy Rule for patient information in all forms, including electronic, paper and spoken patient information.

In addition, a dental practice must have reasonable safeguards in place to limit "incidental" uses and disclosures. An incidental use or disclosure may happen when a dental practice is making a permissible use or disclosure of patient information. For example, a patient may overhear a dentist's confidential conversation with another patient, or may glimpse a patient's information on a sign-in sheet.[18]

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will have in place appropriate administrative, technical and physical safeguards to protect the privacy of patient information. Our dental practice will reasonably safeguard patient information from intentional or unintentional use and disclosure in violation of HIPAA. Our dental practice will reasonably safeguard patient information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure of patient information.

[18] For more information about incidental uses and disclosures, see the Office for Civil Rights, *Incidental Uses and Disclosures*, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html.*

SAMPLE POLICY AND PROCEDURES

Sample Administrative Safeguard Procedures

Sign-in Sheets: After a patient signs in, cover the name with an adhesive opaque strip. Call patients into the exam room by first name only.

Oral communications: Speak quietly when discussing a patient's condition in a waiting room, or other public areas.

Avoid using patients' names in public areas such as hallways and elevators.

Avoid unnecessary disclosures of patient information by monitoring voice levels and being alert for unauthorized listeners. Conduct telephone conversations away from public areas. Use speaker-phones only in private areas.

Telephone messages: Unless a patient has asked not to be contacted by telephone, telephone messages and appointment reminders may be left on answering machines and voicemail systems, but limit the amount of information disclosed in a telephone message.

Faxes: Fax machines must be located in secure areas that cannot be easily accessed by visitors or patients.

Mail: Send mail to the patient's primary address unless the patient requests an alternative address. Postcards may be used for appointment reminders as long as the patient has not objected and the postcard contains the minimum necessary amount of patient information.

Copies: Copies of records containing patient information will be stamped "Copy" in a color other than black so that copies can be distinguished from originals.

Photocopiers and printers: Some printers and photocopiers have built in hard drives. Before our dental practice gets rid of a photocopier or printer (for example, by returning it to a leasing company or donating it), we must confirm whether or not the device has a hard drive. If it has a hard drive, we will have the hard drive securely wiped to prevent unauthorized individuals from accessing any patient information and other sensitive information that may be stored on the hard drive. Some photocopiers and printers include a function that can securely wipe the hard drive. If our device does not have this functionality, or if our device has failed, we will consult with our technical support provider to determine the best way to securely wipe the hard drive.[19]

Destruction of protected health information: When it is appropriate to destroy patient information in compliance with applicable federal and state laws and our practice's document retention policies, the information will be destroyed in way that "secures" it under the breach notification rule.

The Privacy Official will determine when patient information may be disposed of, who may destroy the information, and any safety precautions that apply.

The Privacy Official will ensure that a business associate agreement is in place before our dental practice gives any patient information to a recycling or disposal firm. This includes companies that recycle dental x-rays. Verify the identity of the vendor's representative before turning over any patient information or devices containing patient information unless you know the representative by sight.

[19] For more information about photocopier security visit the Federal Trade Commission, *Copier Data Security: A Guide for Businesses*, *http://business.ftc.gov/documents/bus43-copier-data-security.*

SAMPLE POLICY AND PROCEDURES

The Privacy Official and Security Official will ensure that a business associate agreement is in place with any tech vendor who has access to patient information, including companies that repair, dispose of or wipe electronics containing patient information, and that the disposal or wiping of electronic patient information renders the information "secure" under the Breach Notification Rule.

Sample Physical Safeguards Procedures:

Paper Records: Our practice will store paper records and medical charts away from unauthorized persons. Dental records will be placed face down on desks, counters, and workstations to conceal the identity of patients.

Our receptionist will pull patient dental records the evening prior to the patient visit, and is responsible for ensuring that the records are safely returned to the dental record files.

Patient records may not be removed from the dental office.

Theft or loss of any patient information, including paper records and electronic devices containing patient information, must be reported immediately to the Privacy Official.

Patients and Visitors: Visitors and patients will be appropriately monitored during visits to our practice. Patients will not be allowed to access other patient's records or other patient information.

Sample Technical Safeguard Procedures:

Encryption: Electronic patient information shall be encrypted whenever the Security Official determines that it is reasonable and appropriate to do so. Our practice will consult with our software vendor(s) and Internet provider to determine encryption solutions that would render patient information "secure" under the Breach Notification Rule. Emails sent between our dental practice and other health care providers via a common Internet carrier shall not include patient information unless the email is encrypted.

Internet: Unauthorized access to the Internet from a computer workstation that contains patient information is prohibited.

Our practice will set up a workstation in the lunchroom where workforce members may check personal emails or conduct other personal Internet business.

Portable and Mobile Handheld Computing Devices: Workforce members other than dentists may not store patient information on portable or mobile computing devices. Any patient information on a dentist's portable or mobile handheld computing device must be encrypted in a way that "secures" under the Breach Notification Rule.

Workforce members who store any unsecured patient information on portable or mobile handheld computing devices are responsible for the security of the patient information and are subject to sanctions up to and including termination of employment if the device is misplaced, lost, or stolen. Workforce members must immediately notify the Privacy Official of a breach or suspected breach of protected health information.

Portable Storage Devices: Patient information may not be downloaded onto portable storage devices, such as USB drives and CD-ROMs, unless the device is appropriately encrypted. However, a patient receiving an electronic copy of patient information (Chapter 2, Step 14.1) may request the copy unencrypted on a portable storage device, and our dental practice will provide the copy in that format if requested and if we can readily produce it.

Step 21: De-identification

HIPAA does not apply to properly de-identified information. Properly "de-identify" patient information when appropriate by removing the 18 HIPAA "identifiers" (see list below).

Where to find the rules:

45 CFR 164.502(d)(2);
45 CFR 164.514(a), (b) and (c)

What is required:

HIPAA does not apply to properly de-identified patient information. There are no HIPAA restrictions on the use or disclosure of patient information that has been properly de-identified. If properly de-identified patient information is lost or disclosed to an unauthorized person, breach notification is not required because properly de-identified patient information is not protected by HIPAA.

There are two means of de-identifying patient information:

- The **safe harbor method** requires the removal of 18 specific "identifiers" ***and*** the dental practice's knowledge that the information cannot be used, alone or in combination with other information, to identify the patient.
- The **expert determination method** requires a certain kind of scientist or statistician to analyze the de-identified patient information and determine that the risk of re-identification is very small, and document the methods and result of the analysis

Dental practices probably use the safe harbor method more often than the expert determination method.

Information is not considered de-identified if it is coded and the code is disclosed, or if other means of record identification are disclosed that can be used to re-identify the information.

HIPAA applies to de-identified information that has been re-identified.

A dental practice may use patient information to create de-identified information, or disclose patient information to a business associate who will de-identify the information for the dental practice. If a business associate will de-identify patient information, the dental practice and the business associate must sign a written business associate agreement before the business associate receives the patient information (Chapter 2, Step 13).

Redaction. Redaction (for example, covering up information with a marker) does not make patient information "secure" under the Breach Notification Rule (Chapter 2, Step 22). A dental practice that uses "redaction" may find that the information is not properly de-identified, and that disclosing the information may lead to a breach requiring notification. For example, it might be still possible to read the redacted information, particularly when a redacted paper document is photocopied or scanned.

A dental practice that de-identifies patient information would be prudent to make sure that the method of de-identification is thorough enough that there is a very low probability of compromise under the Breach Notification Rule.

Limited Data Set and Data Use Agreement. For certain research, public health, and health care operations purposes, HIPAA may permit a dental practice to use or disclose patient information with all of the HIPAA identifiers removed except for certain date and location information. This is called a

"limited data set" and it may only be disclosed for certain purposes and only if the recipient has signed a "data use agreement" that contains certain required provisions. While limited data sets and data use agreements are beyond the scope of this book, dental practices should be familiar with the terms, and should obtain legal counsel before using or disclosing limited data sets and/or entering into data use agreements.

The Breach Notification Rule applies to limited data sets. Since limited data sets are not fully de-identified, breach notification is required if an unencrypted limited data set is lost or stolen, or accessed by an unauthorized person, unless the dental practice can demonstrate that there is a low probability that the information was compromised based on a written analysis of the relevant factors, including the four required factors (Chapter 2, Step 22).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our practice will properly de-identify patient information when appropriate.

Sample Procedures

Staff: De-identifying patient information involves removing specific information that can be used to identify a patient. Staff members who have not been trained to de-identify patient information should not attempt to do so.

Privacy Official: HIPAA does not apply to properly de-identified patient information. Using and disclosing properly de-identified patient information when appropriate may help our dental practice avoid HIPAA violations and breaches of unsecured patient information. For example, if we wish to seek the advice of a consultant on a matter involving a patient, providing the consultant with properly de-identified information can minimize the likelihood of a breach. In addition, if the only information we provide to the consultant is properly de-identified, then the consultant is not a business associate and we do not need a business associate agreement with the consultant.

Use the following method to "de-identify" patient information:

1. Remove from the document all of the following "identifiers" for the patient and for the patient's relatives, household members, and employers:

1. Names, including initials
2. Any geographic subdivision smaller than a state (including address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code — the geographic unit formed by combining all zip codes with the same three digits must contain more than 20,000 people; otherwise, the three digit code must be changed to "000.")
3. All elements of dates (except year) for dates directly related to the individual, including birth date, treatment date, lab work date, date of death; and all ages over 89 and all elements of dates (including year) that indicate an age over 89
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers, including the last four digits
8. Medical record numbers

SAMPLE POLICY AND PROCEDURES

9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except that our dental practice may assign a code or other means of record identification to allow the information to be re-identified by our dental practice, as long as:

    i. The code or other means of record identification is not derived from, or related to, information about the individual and is not otherwise capable of being translated so as to identify the individual, and

    ii. Our dental practice does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the code or mechanism for re-identification.

2. The information is not considered de-identified if our dental practice has any actual knowledge that the information could be used, alone or in combination with any other information, to identify an individual who is subject of the information.

3. If we develop a code or other means of re-identifying the information, we must not derive the code from the information about the individual and no one must be able to use the code to identify the individual unless they have the key. We will not use or disclose the code or other means of record identification for any other purpose, and we will not disclose the mechanism for re-identification.

Avoid using redaction to de-identify a document

Remove the identifiers using a method that makes it impossible to read or re-create the identifiers, whether the document being de-identified is in in hard copy or electronic format.

Never use a pencil, pen, marker, etc. to hide the 18 identifiers on a paper document. This is because sometimes the "redacted" information can still be read, particularly if the document is photocopied or scanned. This can lead to a HIPAA violation or a breach. Redaction cannot be used as a method of "securing" patient information under the Breach Notification Rule (Chapter 2, Step 22).

For more information:

Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html*.

Step 22. Breach Notification

A dental practice must implement policies and procedures for complying with the requirements of the Breach Notification Rule. When a dental practice discovers a breach of unsecured patient information, the dental practice must provide timely notice to affected individuals, HHS, and in some cases the media.

Where to find the rules:

45 CFR 164.400 – 45 CFR 164.414

The 2013 Final Rule changed the requirements for Breach Notification. See Chapter 1, Section 2.B. for a discussion of the changes.

What is required:

A dental practice must have breach notification policies and procedures, and must update the policies and procedures as required by HIPAA (for example, when there is a change in the law). When a dental practice discovers a "breach" of "unsecured" patient information, the dental practice must notify the people affected by the breach, HHS, and in some cases the media. The terms "breach" and "unsecured" have special definitions under HIPAA (see below). For example, theft of a laptop containing unsecured patient information may meet the definition of a "breach" even if the thief never accessed the patient information.

Breaches may harm patients and the reputation of the dental practice, and investigating suspected breaches and sending notification can be time-consuming and expensive. It is prudent for a dental practice to take steps to minimize the likelihood of breaches.

In the event of a breach, a dental practice must also comply with other applicable laws, such as state data security laws that are more stringent than HIPAA. For example, some state breach notification laws require faster notification than HIPAA requires.

"Unsecured." HHS has provided a list of approved methods for "securing" patient information (see *The HHS Guidance for Securing Patient Information* below). Electronic patient information is "unsecured" if the file or the device is not properly encrypted. A device (such as a hard drive, laptop or USB drive) can also be secured by proper wiping or destruction.

Since breach notification is not required if electronic information is secured, appropriate encryption is highly recommended. To secure electronic files (for example, Microsoft Word, Excel, Adobe Acrobat, WinZip, etc.), ask your technical support consultant whether the password protection feature built into your version meets the encryption standards in the *HHS Guidance*. For information on securing computers using "Full Disk Encryption," see *Full Disk Encryption Q&A*, Appendix 2.22.4.

Patient information in oral (spoken) form cannot be secured, so notification is required if an oral disclosure that meets the HIPAA definition of a "breach." Hard copy patient information (for example, paper records, photographs, and films) can only be secured through shredding or destruction that makes it impossible to read or reconstruct the information. Although keeping hard copy patient information under lock and key does not "secure" the information for purposes of the breach notification rule, it is prudent to lock up patient information when appropriate in order to minimize inappropriate access and potential breaches.

FIGURE 2.1

The HHS Guidance for Securing Patient Information

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

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

a. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key"[1] and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

   i. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.[2] [3]

   ii. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.[4]

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

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

   ii. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*,[5] such that the PHI cannot be retrieved.

[1] 45 CFR 164.304, definition of "encryption."
[2] NIST Roadmap plans include the development of security guidelines for enterprise-level storage devices, and such guidelines will be considered in updates to this guidance, when available.
[3] Available at *http://www.csrc.nist.gov.*
[4] Available at *http://www.csrc.nist.gov.*
[5] Available at *http://www.csrc.nist.gov.*

"Breach." A "breach" of patient information occurs when the privacy or security of patient information is compromised because someone acquired, accessed, used, or disclosed the information in violation of the Privacy Rule, unless one of three exceptions apply (see *The Three Exceptions to the HIPAA Definition of a Breach* below). Breach notification may be required even if the dental practice does not know for sure that someone accessed the patient information (for example, if an unsecured mobile device containing patient information is lost or stolen, or if paper dental records are disposed of in the regular trash or recycling without securely shredding).

Between September 23, 2009 and September 22, 2013, a dental practice must provide breach notification if an impermissible acquisition, access, use or disclosure of patient information poses a significant risk of financial, reputational, or other harm to the individual.

On or after September 23, 2013, an acquisition, access, use or disclosure of patient information that is not permitted by HIPAA is presumed to be a breach requiring notification. Whenever there is an impermissible use or disclosure of unsecured patient information, a dental practice may choose to provide the required breach notifications without performing a risk assessment. However, a dental practice is not required to provide notification if the dental practice can demonstrate that there is a ***low probability*** that the information has been compromised, based on a written analysis of the relevant factors, including, at 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*, Appendix 2.22.1, includes the four factors and other things to consider when determining whether notification is required.

Business associates. If a dental practice's business associate discovers a breach of unsecured patient information, the business associate must notify the dental practice. The dental practice must provide notification to the people affected by the breach, HHS, and, if required, the media, unless the business associate agreement makes the business associate responsible for providing notification.

When a business associate notifies a dental practice of a breach, the business associate must include, to the extent possible, the identification of each person whose unsecured patient information the business associate knows, or reasonably believes, was accessed, acquired, used or disclosed in the breach, and any other available information that the dental practice must include in the notification letter to individuals. If the business associate does not have this information when it notifies the dental practice, the business associate must provide the information promptly as the information becomes available.

Timeframe. A dental practice must provide notification without unreasonable delay and in no case later than 60 calendar days after "discovery" of the breach. A breach is considered "discovered" on the first day that any workforce member or agent (Chapter 2, Step 13) of the dental practice knows about the breach, or would have known about it if they were "reasonably diligent." In some cases, a dental practice is not deemed to have "discovered" a breach that is only known to the workforce member who committed the breach.

This means that dental practices should take reasonable steps to detect breaches: if a dental practice would have discovered a breach if it had been diligent, the time period may start running on the date the practice *should have* discovered the breach. A dental practice violates HIPAA if it does not provide required notification within the appropriate timeframe. A dental practice should have procedures for

FIGURE 2.2

The Three Exceptions to the HIPAA Definition of a Breach

There are three exceptions to the definition of "breach." One involves the acquisition, access or use of patient information, and the other two involve disclosures of patient information.

i. An unintentional ***acquisition, access, or use*** of patient information by a workforce member of, or person acting under the authority of, the dental practice or a business associate, if the 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 by HIPAA.

   For example: A billing employee of a dental practice receives and opens an email containing patient information that a hygienist mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the hygienist of the misdirected email, and then deletes it.

   In contrast, if a receptionist who is not authorized to access patient information decided to look through patient files in order to learn of a friend's treatment, the impermissible access would not fall within this exception because it was neither unintentional, done in good faith, nor within the scope of the receptionist's authority.

ii. An inadvertent ***disclosure*** by a person who is authorized to access patient information at the dental practice to another person authorized to access patient information at the dental practice, and the information received as a result of disclosure is not further used or disclosed in a way that is not permitted by HIPAA. This exception would also apply if the inadvertent disclosure was by a person authorized to access patient information at a business associate inadvertently disclosed the information to another person authorized to access patient information at the same business associate.

   For example: An assistant inadvertently disclosed patient information to a hygienist that the hygienist is not authorized to access. However, both the assistant and the hygienist are authorized to access certain categories of patient information. The disclosure would not constitute a breach and notification would not be required, provided the patient information is not further disclosed in violation of HIPAA.

iii. A disclosure of patient information where the dental practice 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 the information.

   For example: A dental practice mails some patient statements to the wrong individuals. The statements are returned by the post office, unopened, as undeliverable. The dental practice may conclude that the improper addressees could not reasonably have retained the information. However, if the statements were not returned as undeliverable, and the dental practice knows they were sent to the wrong individuals, the dental practice should either send the required notification, or conduct a written risk assessment to determine if notification must be provided.

   As another example, a dental assistant hands a patient a chart belonging to another patient, but the assistant quickly realizes the mistake and recovers the chart from the patient. If the dental assistant can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.

detecting possible breaches, and train workforce members to be on the alert and *immediately* report suspected breaches of unsecured patient information (for example, to the Privacy Official).

Business associate breach. When a business associate discovers a breach, the business associate must notify the dental practice without unreasonable delay and in no case later than 60 days. In general, a dental practice "discovers" a business associate's breach on the date that the business associate tells the dental practice about the breach. However, if the business associate is an ***agent*** of the dental practice, the dental practice may be deemed to have "discovered" the breach on the day that the agent discovers the breach. ***This means that if a business associate is an agent, the timeframe for providing breach notification may be much tighter than if the business associate is not an agent.***

Law enforcement delay. A law enforcement official can delay notification by telling the dental practice or business associate that notification would impede a criminal investigation or cause damage to national security. If the law enforcement official's statement is in writing and specifies the timing of the delay, the dental practice or business associate must delay notification for that amount of time. If the law enforcement official's statement is made orally, the dental practice or business associate must document the statement, including the identity of the law enforcement official, and delay notification for no longer than 30 days unless the law enforcement official provides a written statement that says how long the delay must last.

Assessing possible breaches. As of September 23, 2013, when a dental practice discovers a breach of unsecured patient information, the dental practice may choose to notify affected individuals, HHS, and, if required, the media without performing a risk assessment. In the alternative, a dental practice may perform a written assessment to determine whether there is a low probability that the information has been compromised based on an analysis of the relevant factors, including, at a minimum, the required four factors (see above, and *Sample Breach Assessment Form*, Appendix 2.22.1). If the dental practice cannot demonstrate a low probability of compromise, the dental practice must provide the required notification. The risk assessment must be ***in writing*** because the dental practice (or business associate, as appropriate) must be able to prove to HHS that either all required notifications were made or that the use or disclosure did not constitute a breach.

Providing notification to individuals. The Breach Notification Rule spells out the required content of the notice, how notice must be provided, and what to do if a dental practice does not have contact information for any of the people affected by the breach.

Content. The notice must be written in plain language, and must contain, to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known,

2. A description of the types of unsecured patient information involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved). The notice should not repeat the breached information — it should merely provide a description,

3. Any steps patients should take to protect themselves from potential harm resulting from the breach,

4. A brief description of what the dental practice is doing to investigate the breach, to mitigate harm to patients, and to protect against any further breaches, and

5. Contact procedures for patients to ask questions or learn more information. This must include a toll-free telephone number, an email address, website, or postal address.

Notice to individuals. In general, a dental practice must send notice to individuals by first-class mail at their last known address. However, a dental practice can email notice to patients who have agreed to electronic notice and haven't withdrawn their agreement. Since email may be faster and less expensive than first-class mail, a dental practice may wish to ask patients agree to receive electronic notice (see *Sample Agreement to Receive Electronic Communication,* Appendix 2.22.3).

A dental practice may send more than one communication as information about the breach becomes available.

If a breach involves information of a patient who is deceased, the dental practice must send notification to the patient's next of kin or personal representative if the dental practice has that person's address.

Substitute notice. In some cases, a dental practice will not have sufficient or up-to-date contact information for one or more persons affected by the breach, so the dental practice must provide "substitute notice." If a dental practice does not have sufficient or up-to-date contact information for the next of kin or personal representative of a deceased patient, the dental practice is not required to provide substitute notice.

For nine or fewer persons: If the dental practice has insufficient or out-of-date contact information for nine or fewer individuals, the dental practice must provide notice by telephone, an alternative form of written notice, or other means that is reasonably calculated to reach the individuals.

For 10 or more persons: A dental practice that has insufficient or out-of-date contact information for 10 or more individuals may use a conspicuous posting on the home page of the dental practice's website for 90 days. In the alternative, the dental practice may place a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside (the dental practice must generally purchase media notice for substitute notice purposes).

Whether substitute notice is for nine or fewer or for ten or more individuals, the notice must include a toll-free phone number that remains active for at least 90 days where people can learn whether their patient information was involved in the breach.

Urgent notice: If the dental practice decides that urgency is required because there is an imminent possibility that the breached information could be misused, the dental practice may call people on the phone or reach them by another means, ***in addition to*** sending the required breach notification.

State law. Many states have breach notification laws and other data security laws. For example, state law may require notification if there is a breach of electronic data containing a person's name and one or more of the following: Social Security number, credit or debit card number, driver's license or state I.D. number, or account number. State law may require that notice be provided within an even shorter time frame than HIPAA requires. Dental practices should be familiar with their state law requirements and make sure their breach notification policies and procedures comply with both HIPAA and applicable state law. HIPAA does not pre-empt state law that is more stringent than HIPAA (for example, state law that requires more protection of patient information or that gives patients more rights over their health information).

Providing notice to HHS. In addition to notifying the people affected by the breach, a dental practice must notify HHS. Forms and instructions for notifying HHS are at *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html*.

500 or more. If a breach involves 500 or more persons, the dental practice must notify HHS without unreasonable delay and in no event later than 60 calendar days after discovery of the breach, unless there is a law enforcement delay (see above). Information about reported breaches involving 500 or more persons is posted on the HHS website: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html*.

Fewer than 500. A dental practice must keep a log of breaches involving 499 or fewer individuals that occur during each calendar year, and must submit the information to HHS no later than 60 days after the end of each calendar year (approximately March 1). (See *Sample Breach Log*, Appendix 2.22.2.)

Providing notice to the media. If a breach involves more than 500 residents of a state or jurisdiction, a dental practice must notify prominent media outlets serving the state or jurisdiction. Media notice, which is generally in the form of a press release, must be made without unreasonable delay and in no case later than 60 calendar days after discovery of the breach, unless there is a law enforcement delay (see above).

Here are examples of possible breaches:

- A dentist inadvertently leaves an unencrypted smartphone with electronic patient information on a store counter.
- A thief breaks into a dentist's car or home or practice and steals a laptop, tablet or desktop with unencrypted patient information.
- A dental practice disposes of insufficiently shredded paper documents containing patient information in the regular trash or recycling.
- A hacker or disgruntled employee accesses patient information such as Social Security numbers or credit card numbers.
- A dental practice workforce member looks at a patient's file out of curiosity.
- A dental practice workforce member mentions patient information to a friend or family member.
- A dental practice workforce member takes paper patient information out of the dental practice to work on at home and leaves the documents on the train.
- A dental practice workforce member emails unencrypted patient information to the wrong email address.
- A dental practice workforce member sends an email to a group of patients and enters all of the patients' email addresses in the "send" field, rather than sending the email to the dental practice itself and blind copying all of the patients.
- A hacker obtains a patient's dental plan information and other information about the patient, and uses the information to obtain dental care for himself or a family member.

For more information about the HIPAA Breach Notification Rule, visit the OCR website: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html*.

ADA® TIP

To avoid most situations requiring notification of a breach of electronic protected health information, encrypt your electronic data in storage, in transit and on mobile devices. When it is appropriate to destroy patient information in any form, make sure it is destroyed so that it the patient information is secured (see The HHS Guidance for Security Patient Information above).

ADA TIP

Before a breach occurs, a dental practice is prudent to investigate any vendors and professionals whose assistance our dental practice may require in the event of a breach of unsecured patient information, and select and develop relationships as appropriate. Such vendors and professionals may include technical advisors who could investigate and perform forensic analysis in the event of a suspected breach of electronic patient information, a 24-hour service that could respond to calls on the toll-free number in case the dental practice must provide substitute notice to 10 or more individuals, and a qualified attorney in to advise the dental practice on the requirements of HIPAA and other applicable laws, such as state data security law.

SAMPLE POLICY AND PROCEDURES

Sample Policy

When our dental practice or one of our business associates discovers a possible breach of unsecured patient information, our dental practice will investigate and provide timely notification in compliance with HIPAA and applicable state law, unless our dental practice can demonstrate, through an appropriate assessment of the relevant factors, including the four required factors, that there was a low probability that the information has been compromised.

Sample Procedures

Staff: Be alert for possible breaches, and notify the Privacy Official ***immediately*** if you suspect a breach has occurred. Following our dental practice's Privacy and Security policies and procedures can help minimize possible breaches of unsecured patient information.

Privacy Official: Develop appropriate breach notification policies and procedures and put them into action. Update the policies and procedures when appropriate, such as when there is a change in the law. Train our workforce members to comply with the policies in procedures. In particular, train workforce members to notify you ***immediately*** if they even suspect that a breach of unsecured patient information may have occurred. Train staff to follow our dental practice's Privacy and Security Policies and procedures to minimize possible breaches of unsecured patient information.

Investigating and assessing possible breaches. If you discover a possible breach, or if a workforce member or a business associate tells you about a possible breach, investigate immediately. If a breach of unsecured patient information has occurred, our dental practice may choose to provide the required notifications without performing a risk assessment. However, notification is not required if our dental practice can demonstrate that there is a low probability that the information has been compromised, based on an analysis of the relevant factors, including the four factors required under the Breach Notification Rule. Document the analysis using our Breach Assessment Form (see *Sample Breach Assessment Form*, Appendix 2.22.1).

SAMPLE POLICY AND PROCEDURES

Sending notification. If notification is required, draft notice letters that comply with HIPAA and other applicable law, and provide timely notice (complying with any applicable law enforcement delay) to affected individuals, HHS, and, if required, to the media. Breaches involving 500 or more individuals must be reported to HHS without unreasonable delay and in no event later than 60 days after discovery of the breach. Maintain a log of all breaches involving fewer than 500 individuals and submit the log annually to HHS (see *Sample Breach Log*, Appendix 2.22.2).

Substitute notice: If we lack contact information for nine or fewer individuals involved in a breach, contact them via phone or using another means reasonably calculated to reach them. Do not provide patient information to an unauthorized person when providing substitute notice.

If we lack contact information for 10 or more individuals affected by a breach, determine whether to post a conspicuous notice about the breach on the homepage of our website for 90 days, or to provide a conspicuous notice in major print or broadcast media in the area where the affected individuals likely reside, then provide the substitute notice. Either form of notice must direct individuals to a toll-free telephone number that is active for at least 90 days that people can call to find out if their information was involved in the breach.

Electronic communications: Determine whether asking patients to sign agreements permitting electronic communications would help the dental practice notify patients in the event of a breach of unsecured patient information. If so, develop an agreement to receive electronic communications (see *Sample Agreement to Receive Electronic Communication*, Appendix 2.22.3) and develop and implement a process for requesting patient signatures and maintaining a record of the patients who have signed the agreement and an up-to-date record of the patients' email addresses, and a record of patients who have withdrawn their agreement to receive electronic communications.

Documentation: Retain all documentation related to our dental practice's compliance with the Breach Notification Rule for at least six years from the date the document was created, or from the date the document was last in effect, whichever is later (Chapter 2, Step 19). Examples of breach notification documentation includes policies and procedures, breach assessment forms, copies of notification letters, logs, media notices, and press releases.

ADA TIP

When it is legally appropriate to dispose of patient information, use disposal methods that render the information secure under the Breach Notification Rule. In accordance with the *HHS Guidance*, select appropriate methods for secure disposal of hard copy and electronic patient information, and for secure disposal of electronic media that contains patient information.

ADA® TIP

To avoid breaches of unsecured patient information, encrypt electronic patient information in storage, in transit, and on mobile devices, and train staff as appropriate to use proper encryption methods. Breaches can also be avoided by encrypting all dental practice computers and laptops using Full Disk Encryption that meets the standards in the *HHS Guidance* (see *Full Disk Encryption Q&A*, Appendix 2.22.4). Avoid using USB drives and CD-ROMs to store patient information because they are easy to lose and difficult to encrypt; *however*, a patient who requests a copy of his or her information that a dental practice maintains in an electronic designated record set may request that it be provided on a USB drive or CD-ROM (Chapter 2, Step 14.1). A dental practice may determine, through a written risk assessment, that using outside USB drives and CD-ROMs poses an unacceptable level of risk, and may have a supply of these devices on hand to provide electronic copies.

Sample Forms:

- *Sample Breach Assessment Form*, Appendix 2.22.1
- *Sample Breach Log*, Appendix 2.22.2
- Sample Agreement to Receive Electronic Communication, Appendix 2.22.3
- *Full Disk Encryption Q&A*, Appendix 2.22.4

Government Resources:

Office for Civil Rights, *Breach Notification Rule*, *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html*.

Appendix 2.22.1
Sample Breach Assessment Form

This sample form illustrates how a dental practice might assess suspected breaches of unsecured protected health information.

A. DESCRIBE THE INCIDENT:

- Date the suspected breach was discovered:
- Date the suspected breach occurred:
- Brief statement of what happened:
- How we learned of the breach:
- Describe the kind of information involved:
- Describe the people and entities involved:
- If the incident involved a *use*[1] of information:
    - Who used the information?
    - For what purpose?
- If the incident involved a *disclosure*[2] of information:
    - Who disclosed the information?
    - To whom?
    - For what purpose?
- Describe the format of the information (e.g., paper records, films, electronic):
- If electronic information was involved:
    - Was the electronic information in storage? (e.g., on a desktop computer hard drive, a laptop, a CD or a USB drive)
    - Was the electronic information in transit? (e.g., in an email or through a portal)
    - Was the electronic information appropriately encrypted?
    - Was the password of an authorized person/entity used to access the information?
- What is being done to mitigate any risk to the privacy and security of the information?

B. IF ANY OF THE FOLLOWING APPLY, HIPAA DOES NOT REQUIRE NOTIFICATION:[3]

1. If the information was properly "secured" using a method approved by the U.S. Department of Health and Human Services ("HHS"):

   Was the information "secured"? ☐ Yes ☐ No
   If yes, explain: _____

   _____

[1] HIPAA defines "use" as the sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains the information.
[2] HIPAA defines "disclosure" as the release, transfer, provision of access to, or divulging any manner of information outside the entity holding the information.
[3] However, other applicable law may apply, such as state or local data security laws.

2. If the information was not "protected health information" ("PHI") as defined by HIPAA.[5]

   Was the information PHI? ☐ Yes ☐ No
   If no, explain:_____

   _____

3. If the use or disclosure was permitted or required under the HIPAA Privacy Rule.

   Was the use or disclosure permitted or required? ☐ Yes ☐ No
   If yes, explain: _____

   _____

4. If the use or disclosure was authorized by the patient in compliance with the HIPAA Privacy Rule.[6]

   Did the patient appropriately authorize the use or disclosure? ☐ Yes ☐ No
   If yes, attach a copy of the signed authorization form.

5. If any of the following exceptions apply:

   Exceptions 1:

   - The incident involved unintentional acquisition, access or use of PHI by a workforce member, or by an individual or entity acting under the authority of the dental practice or one of its business associates,
   - The acquisition, access or use was made:
     - In good faith, and
     - Within the scope of authority, and
   - The acquisition, access or use does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule.

   Exception 2:

   - The incident involved an inadvertent disclosure:
     - by an individual or entity that is authorized to access PHI at the dental practice (or one of its business associates),
     - to another person authorized to access PHI at the dental practice (or the same business associate), and
   - The information received as a result of such disclosure was not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

[5] Information, including demographic and genetic information, is PHI if it:
- Is in any format, including oral, electronic, or hard copy (e.g., paper, film or photograph),
- Was created or received by a health care provider, health plan, employer, or health care clearinghouse,
- 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
  - Includes one of the 18 HIPAA identifiers (see Chapter 2, Section 2.2.8 of *The ADA Practical Guide to HIPAA Compliance Privacy and Security Manual*), or if there is a reasonable basis to believe the information can be used to identify the individual, unless
- The information is:
  - Employment records held by the dental practice in its role as an employer
  - Education records covered by the Family Educational Rights and Privacy Act ("FERPA")
  - Information regarding an individual who has been deceased for more than 50 years.

[6] See "Authorization," Section 2.2.7, Chapter 2, of *The ADA Practical Guide to HIPAA Compliance Privacy and Security Manual.*

Exception 3:

- The incident involved a disclosure of PHI, and
- The dental practice or business associate (as applicable) has a good faith believe that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Does one of the three above exceptions apply? ☐ Yes ☐ No
If yes, explain: _____

_____

C. RISK ASSESSMENT:

If the information was unsecured PHI, and

- the use or disclosure was not permitted or required under HIPAA,
- the individual did not appropriately authorize the use or disclosure, and
- none of the exceptions above apply,

then the dental practice must send timely breach notification unless the dental practice demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of the relevant factors, including at least the following factors:

Factor 1: The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

Assessment:

Factor 2: The unauthorized person who used the protected health information or to whom the disclosure was made.

Assessment:

Factor 3: Whether the PHI was actually acquired or viewed.

Assessment:

Factor 4: The extent to which the risk to the PHI has been mitigated.

Assessment:

Should any additional relevant factors be considered in determining the probability that the PHI has been compromised? If so, describe:

_____

_____

Assessment:

Based on a risk assessment involving all of the above factors, is there an overall low probability that the PHI has been compromised?

- **The probability of compromise is LOW:** _____
- **The probability of compromise is NOT LOW:** _____

IF THE PROBABILITY THAT PHI HAS BEEN COMPROMISED IS NOT LOW, HIPAA BREACH NOTIFICATION IS REQUIRED.

Is notification required under other applicable federal, state or local law? ☐ **Yes** ☐ **No**

If yes, explain: _____

_____

_____

This risk assessment form is accurate and complete.

Signed: _____

Name: _____

Title: _____ Date:_____

Appendix 2.22.2

Sample Breach Log

This sample form illustrates how a dental practice might log breaches that affect less than 500 individuals for annual submission to the U.S. Department of Health and Human Services. The following information must be recorded for every breach of unsecured patient information.

Date of breach: _____

Date breach was discovered:_____

Did the breach occur at or by a business associate?

- ☐ Yes
- ☐ No

If yes:

Name of business associate: _____

Address: _____

City:_____ State: _____ Zip code: _____

Business associate contact name:_____

Business associate contact phone number:_____

Business associate contact email:_____

Approximate number of individuals affected by the breach: _____

Type of breach:

- ☐ Theft
- ☐ Loss
- ☐ Improper disposal
- ☐ Unauthorized access or disclosure
- ☐ Hacking or information technology incident
- ☐ Unknown
- ☐ Other: _____

Where was the breached information located?

- ☐ Laptop
- ☐ Desktop computer
- ☐ Network server
- ☐ Email
- ☐ Other portable electronic device
- ☐ Other
- ☐ Electronic medical record
- ☐ Paper

Type of patient information involved:

- ☐ Demographic information
  - o Name
  - o Social Security number
  - o Address or zip code
  - o Driver's license number
  - o Date of birth
  - o Other identifier
- ☐ Financial information
  - o Credit card or bank account number
  - o Claims information
  - o Other financial information
- ☐ Clinical information
  - o Diagnosis or conditions
  - o Lab results
  - o Medications
  - o Other treatment information
- ☐ Other

Brief Description of the breach (include the location of the breach, a description of how the breach occurred, and any additional information regarding the type of breach, type of media, and type of protected health information involved in the breach):

_____

_____

_____

What safeguards (protective measures) were in place prior to the breach:

- ☐ Firewalls
- ☐ Packet filtering (router-based)
- ☐ Secure browser sessions
- ☐ Strong authentication
- ☐ Encrypted wireless
- ☐ Physical security
- ☐ Logical access control
- ☐ Anti-virus software
- ☐ Intrusion detection
- ☐ Biometrics

Date(s) notice was provided to affected individual(s):

Date first notice was sent:

Month: _____ Day: _____ Year: _____

Date last notice sent:

Month: _____ Day: _____ Year: _____

Was substitute notice required? (Substitute notice is required if you lack sufficient or up-to-date contact information for any affected individuals)

☐ Yes

☐ No

Was media notice required? (Media notice is required if a breach involves 501 or more residents of a state or jurisdiction)

☐ Yes

☐ No

What action did the dental practice take in response to the breach?

☐ Security and/or privacy safeguards

☐ Mitigation (actions to lessen the harm of the breach to affected individuals)

☐ Sanctions (against workforce members who violated the policies and procedures)

☐ Policies and procedures

☐ Other

If "other," please describe: _____

Describe in detail any additional actions taken following the breach:

_____

_____

_____

_____

This form provides for the recording of the information required by the Office for Civil Rights ("OCR") when submitting reports of breaches. See OCR, *Notice to the Secretary of HHS of Breach of Unsecured Protected Health Information http://ocrnotifications.hhs.gov.* **This material is for general reference purposes only and does not constitute legal advice. It covers only HIPAA, not other federal nor state law. Changes in applicable laws or regulations may require revision. Dentists should contact qualified legal counsel for legal advice, including advice pertaining to HIPAA compliance, the HITECH Act, and the U.S. Department of Health and Human Services rules and regulations.**

Appendix 2.22.3

Sample Agreement to Receive Electronic Communication

This sample form illustrates how a dental practice might obtain patient agreement to receive communications via email.

Patient Name: _____ Date of Birth: _____

I agree that the dental practice may communicate with me electronically at the email address below.

I am aware that there is some level of risk that third parties might be able to read unencrypted emails.

I am responsible for providing the dental practice any updates to my email address.

I can withdraw my consent to electronic communications by calling:

_____**[practice's telephone number]**.

Email Address (PLEASE PRINT CLEARLY):

_____@_____

Patient Signature: _____ Date:_____

Appendix 2.22.4
Full Disk Encryption Q&A

INTRODUCTION

Why encrypt?
When electronic patient information is properly encrypted, HIPAA does not require breach notification even if the device that stores the information is lost or stolen, as long as the encryption key (e.g., the password) is not compromised. For example, if a covered dental practice stores patient information on a laptop computer and the laptop is stolen, the dental practice does not need to send breach notification if the dental practice can demonstrate that the laptop is properly encrypted and the encryption key is secure.

How to encrypt?
A variety of methods can be used to encrypt data "at rest" (i.e., stored data) or data "in transit" (such as an email). **This resource only discusses encrypting data at rest using the method known as "full disk encryption" ("FDE")**. A variety of FDE products are available. Several products are discussed below as examples only.

Are there risks to using FDE?
Yes. Remembering your password is crucial when your computer is protected with FDE. ***If you forget your password you may not be able to recover your data!*** Securely backing up your data may also help with recovery (see below). Whether or not you back up your data, it is important to ***protect your password.*** If both a properly encrypted computer and the password are stolen, HIPAA may require breach notification even though proper encryption was used.

What is "Full Disk Encryption" (or FDE)?
- It is a security tool that unobtrusively encrypts your entire computer hard drive
- This encryption secures your hard drive so that no one can access it without a valid password.
- This tool becomes important to you if your computer is lost or stolen.

The password you already use to log onto your computer isn't enough. Why not?
- Password protection alone does not "secure" patient information under the HIPAA Breach Notification Rule.
- Unfortunately, Windows and Macintosh passwords offer only limited protection of your data. If a computer protected only with a password is stolen, HIPAA may require sending breach notification.
- Even though your computer is protected by a password, it is still relatively easy for someone to access your data. They don't need to know your password to do so. They only need physical access to your computer and a little bit of technical knowledge.
- One way is to boot another operating system from your CD-ROM drive or from a USB drive. For example, a person who has your computer can boot a copy of Linux from CD-ROM and then access your Windows or Macintosh hard drive the same way you would access any USB drive.
- Another way is to remove your hard drive from your computer and temporarily attach it to another computer, again sort of like a USB drive.
- In either case, any file on your computer could be accessed without your permission or knowledge, if someone had possession of your computer.

Using "Full Disk Encryption" is a simple way to prevent someone who steals your computer from accessing any patient information on the computer.

How Full Disk Encryption works
- You first obtain Full Disk Encryption software and install it.
- The software uses a password that you provide to encrypt your entire computer's hard drive.
- When you start up your computer, you may be prompted for a boot up password (this is an option for some software). If not, you will be prompted for your usual login password (which should also be a strong password — see "Strong Passwords" below).
- If a person tries to boot another operating system and access your files, they will not be able to see any data because they do not have the encryption password.
- If a person removes your hard drive and tries to access the files, they will not be able to see any data because they do not have the encryption password.

- In order to access a hard drive that has been encrypted using Full Disk Encryption, you need to know either the encryption password or a valid login password, depending on the configuration.

Where can I obtain Full Disk Encryption software?

There are any number of appropriate products available, but here are a few examples:

- If you're using the Pro Enterprise editions of Windows 8 or later, or Windows 7 Ultimate or Enterprise, or Vista Ultimate or Enterprise, you can enable the built in Bitlocker software, which provides Full Disk Encryption.
- If you're a Macintosh user, the versions of Apple's OS X called "Yosemite" and "El Capitan" include an enhanced version of a tool called FileVault. FileVault includes Full Disk Encryption functionality. OS X Yosemite was released in October 2014 and El Capitan was released in June 2015.
- Another product available for either Windows or Macintosh computers is Symantec's PGP Whole Disk Encryption. This software costs about $100 per computer.

If you wish to use FDE software, make sure that the FDE software complies with one of these standards:

- It is FIPS 140-2 (Federal Information Processing Standards) validated. We are unaware of any FDE software that is not FIPS 140-2 validated, but you should verify.
- Alternately, confirm that your FDE software uses AES encryption with 128 bit keys or longer.

After you've installed Full Disk Encryption:

- Don't forget your FDE password. If you do, you may lose data.
- Do regular backups of the computer protected with FDE. This is a good idea under any circumstances, but if you have a hard drive failure, it may be impossible for a hard drive recovery service to recover your data files even though you've provided the FDE password.
- When you perform those backups, be sure to encrypt them using a strong password and AES 128 bit encryption at a minimum.

If you previously encrypted your computer using TrueCrypt, you should investigate other FDE products. TrueCrypt was discontinued in May of 2014, and support is no longer available. Therefore, this software is no longer a source for FDE.

If the application you're using to store patient information (such as a Dental Practice Management system) encrypts that data within the application, FDE may not be required to avoid breach notification in the event of the theft or loss of a computer. However, using FDE in this situation provides a second level of security.

Strong Passwords

A strong password is not easy to guess. Suggestions for constructing a strong password:

- Make the password at least eight characters long (ten or twelve is even better)
- Use upper and lower case letters, numerals, and punctuation symbols
- Do not use:
  - Words that can be found in a dictionary (English or foreign language) or words from fictional languages, names of famous people, famous fictional characters, and so forth
  - Words that are part of your name
  - Doubling up of words (such as "golfgolf")
  - Patterns such as "12345678," "qwerty," "asdfgh," etc.
  - Prefixing or suffixing any word found in sources listed above with numbers (for example, "1password" or "password1")
  - A commonly used sentence or song lyric, such as "To be or not to be," or "Oh say can you see."

Changing passwords regularly, and never reusing old passwords, helps protect data.

Data can be compromised if an unauthorized person obtains or guesses a password — for example, if a password is easy to guess or is not a "strong password," if someone posts a password on a computer or stores it in a laptop case, or if someone stores passwords electronically in an unencrypted Microsoft Word document.

Step 23: Complaints

Respond appropriately when anyone complains about the dental practice's privacy or breach notification practices.

Where to find the rules:

45 CFR 164.530(d)
45 CFR 164.530(a)(1)
45 CFR 164.520(b)(1)(vi)
45 CFR 160.306

What is required:

Anyone (not just patients) has the right to complain about a dental practice's HIPAA compliance to the dental practice or to the federal government. A dental practice must designate a contact person who is responsible for receiving those complaints. This could be the Privacy Official (Chapter 2, Step 1, and *Sample Designation of Privacy Official*, Appendix 2.1.1). A dental practice must also have a process in place for people to make complaints about the dental practice's:

- privacy and breach notification policies and procedures,
- compliance with its policies and procedures, or
- compliance with the HIPAA Privacy Rule or the Breach Notification Rule.

A dental practice must document all complaints received and their "disposition," if any (for example, how the dental practice may have followed up on the complaint) (see *Sample Complaint Log*, Appendix 2.23).

HIPAA prohibits dental practices and business associates from intimidating or retaliating against anyone for filing a complaint (Chapter 2, Step 17).

The Notice of Privacy Practices (Chapter 2, Step 3) must state that people may complain to the dental practice and to the Secretary of HHS if they believe their privacy rights have been violated. The Notice must briefly describe how people can file a complaint with the dental practice, and must state that people will not be retaliated against for filing a complaint (see *Sample Notice of Privacy Practices*, Appendix 2.3.1).

If a dental practice denies a patient's request to see or get copies of patient information (Chapter 2, Step 14.1) or to make a change to information (Chapter 2, Step 14.2), the denial letter must have (among other things) a description of how the person may complain to the dental practice or HHS, including the name or title and telephone number of the contact person at the dental practice (see *Sample Request for Access*, Appendix 2.14.1, and *Sample Request for Amendment*, Appendix 2.14.2.1).

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will provide a process for complaints about our HIPAA Privacy and Breach Notification policies, procedures, and compliance. Our practice will document any complaints received and their disposition, if any.

Sample Procedures

Staff: The Privacy Official is responsible for receiving and processing complaints about our dental practice's privacy practices. If anyone complains to you about the privacy of patient information at our dental practice, or about how our dental practice complies with HIPAA, immediately put the person in touch with the Privacy Official.

Privacy Official: You are designated to receive complaints about the privacy of patient information at our dental practice and about how our dental practice complies with HIPAA. When anyone makes a complaint, you must:

- receive the complaint (for example, by listening if the complaint is oral, or by reading the complaint if it is in writing)
- enter the time, date, and a brief description of the complaint into our complaint log (see *Sample Complaint Log*, Appendix 2.23)
- Determine the appropriate disposition of the complaint (for example, any required follow-up). For example,
    - Should a sanction (disciplinary action) be applied against a workforce member who violated a policy or procedure?
    - Should an unauthorized disclosure be logged in case a patient asks for an accounting of disclosures? (Chapter 2, Step 14.3)
    - Has there has been a breach of unsecured patient information requiring notification? (Chapter 2, Step 22)

Retain all documentation related to complaints for at least six years from the date the document was created, or six years from when the document was last in effect, whichever is later. (Chapter 2, Step 19)

At no time will our practice retaliate against an individual for filing a HIPAA complaint.

Sample Forms:

- *Sample Complaint Log*, Appendix 2.23

For more information:

Office for Civil Rights, *How to File a Complaint*, *http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html*

Appendix 2.23
Sample Complaint Log

This sample form illustrates how a dental practice might log complaints about the dental practice's privacy practices or HIPAA compliance.

Complaint	Name and contact information of the person making the complaint	Date complaint was made	Date response sent to person who made the complaint	Sanctions, if any	Describe any changes resulting from the complaint i.e. training, process redesign

Step 24: Fundraising

Special HIPAA rules apply to the use and disclosure of patient information for fundraising purposes.

Where to find the rules:

45 CFR 164.514(f)
45 CFR 164.520(b)(1)(iii)(A)

The 2013 Final Rule changed the requirements for fundraising. See Chapter 1, Section 2.K. for a discussion of the changes.

What is required:

While most dental practices are unlikely to use or disclose patient information in connection with a fundraising campaign, dental practices should be aware that HIPAA imposes restrictions on fundraising activities that involve patients and/or patient information.

In general, a dental practice cannot use or disclose patient information for fundraising purposes without the written authorization of the patient. However, special HIPAA rules apply to a dental practice that wishes to use or disclose patient information to raise funds for the dental practice itself, when appropriate (for example, if the dental practice is a nonprofit corporation).

A dental practice that wishes to use or disclose patient information to raise funds for the practice does not need to have each patient who receives a fundraising communication sign an authorization form (Chapter 2, Step 9) ***if*** the dental practice:

- only uses or discloses permitted categories of patient for the fundraising purpose,
- permits people to opt out of receiving further fundraising communications,
- includes information about the opt-out method in each fundraising communication, and
- includes a statement in the Notice of Privacy Practices that the dental practice may contact the patient to raise funds for the dental practice and that patients have a right to opt out of receiving such communications.

The opt-out process must not create an undue burden on the patient or cost more than a nominal amount (for example, requiring people to write and send a letter via U.S. mail would be too burdensome, but requiring patients to mail a pre-printed postcard would not create an undue burden under HIPAA).

The dental practice cannot condition treatment or payment on whether the person opts out.

Sending a fundraising communication to a person who has opted out is a HIPAA violation.

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will obtain appropriate patient authorization when required before using or disclosing patient information for fundraising purposes.

Sample Procedures

Staff: Do not make fundraising requests to patients, or use or disclose patient information for any purpose involving fundraising, unless our dental practice has received appropriate authorization, when required.

Privacy Official: Train staff not to make fundraising requests to patients, nor use or disclose patient information for fundraising purposes, unless our dental practice has received appropriate authorization when required.

If our dental practice wishes to use or disclose patient information to raise funds for a charitable purpose, and patient authorization is required for the use or disclosure, ensure that every patient whose information is used or disclosed has signed an appropriate authorization form.

If our dental practice wishes to use or disclose patient information to raise funds for the practice itself, ensure that the requirements of 45 CFR 164.514(f) and 45 CFR 164.520(b)(1)(iii)(A) are met, and train staff to comply with the applicable procedures.

Sample Forms:

- *Sample Notice of Privacy Practices*, Appendix 2.3.1

Step 25: Review and Revise

Keep your privacy program up to date by reviewing periodically and revising whenever appropriate.

Where to find the rules: Step 25.

45 CFR 164.530(i)

What is required:

A dental practice must revise its HIPAA Privacy and Breach Notification policies and procedures from time to time as necessary to remain in compliance with the HIPAA Rules. (Chapter 2, Step 2) When there is a change in the HIPAA Rules, or a change at the dental practice that affects the dental practice's HIPAA compliance, the dental practice must promptly document and implement the revised policies and procedures.

Examples of events that may require revisions include:

- HHS issues new HIPAA rules
- A change in the type of the dental practice's activities that relate to patient information
- The dental practice obtains new technology that require revised policies and procedures for safeguarding patient information
- The dental practice makes a change that materially affects the content of the Notice of Privacy Practices (Chapter 2, Step 3)

SAMPLE POLICY AND PROCEDURES

Sample Policy

Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA.

Sample Procedures

Staff: From time to time our dental practice may revise our privacy and breach notification policies and procedures (for example, if the HIPAA rules change). Staff must comply with new policies and procedures as they are implemented.

Privacy Official: Revise our dental practice's privacy and breach notification policies and procedures as appropriate so that our dental practice remains in compliance with HIPAA.

When our Policies and Procedures are revised, train our workforce to comply with the new policies and procedures.

If a change affects our Notice of Privacy Practices, revise the Notice and provide the revised Notice as appropriate (Chapter 2, Step 3).

Document any changes to our HIPAA policies and procedures, and retain both the new and the old policies and procedures for at least six years from the date the document was created or the date when the document was last in effect, whichever is later (Chapter 2, Step 19).