Policies and Procedures
For The Dental Practice of Dr. Bryan Randolph

Step 1: Privacy Official

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.

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.

Step 2: Privacy Policies and Procedures

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.

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.

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

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.

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 (either signed by the patient or completed by staff), then at that patient's next appointment give the patient a copy of the Notice and ask the patient to sign the acknowledgement form.

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.

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.

Step 4: Designated Records Sets

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.

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.

Step 5: Minimum Necessary

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.

Procedures

Staff: Do not access patient information that 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.

Step 6: Verify Identity

Policy

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

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.

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:

- 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

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).

Step 7: Required Disclosures

Policy

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

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.

Step 8: Permitted Uses and Disclosures

Policy

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

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.

Step 9: Patient Authorization Forms

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.

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.

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 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 has requested an 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.

Step 10: Subsidized Marketing Communications

Policy

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

Procedures

Staff: Unless approved by the Dentist and the Privacy Official, 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

Step 11: Sale of Patient Information

Policy

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

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

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.

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 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).
-

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, in consultation with the Dentist and legal counsel (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, work with the dentist and legal counsel to 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).

Step 13: Business Associates

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.

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.

Step 14: Patient Rights and Requests

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.

Procedure

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 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.

Step 14.2: Amendment

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 send a copy of the amended information to 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.

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.

A patient may ask to make a "request for amendment," or a patient might say instead "this information is wrong" or "I want you to change this." Be alert for requests to amend records, however they are worded.

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).

Future disclosures of the information:
If the patient gives us a statement of denial, 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 for log all requests for amendment and their disposition (see *Sample Amendment Request Log,* Appendix ***), 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).

Step 14.3: Accounting of Disclosures

Policy

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

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.

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.

Step 14.4: Confidential Communications

Policy

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

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.

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).

Step 14.5: Restricted Disclosure

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.

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).

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.

Step 15: Training

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.

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.

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.

Step 16: Disciplinary Actions ("Sanctions")

Policy

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

Procedures

Staff: Our dental practice applies appropriate sanctions against workforce members who violate our HIPAA privacy 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

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.

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
- 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

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.

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

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.

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

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.

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. .[1]

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.

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.

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.

[1] 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.

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.

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. E-mails sent between our dental practice and other health care providers via a common Internet carrier shall not include patient information unless the e-mail is encrypted.

Internet: Unauthorized access to the Internet from a computer workstation that contains patient information is prohibited.

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

Policy

Our practice will properly de-identify patient information when appropriate.

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
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

Policy

When our dental practice or one of our business associates discovers a possible breach of unsecured patient information, our dental practice will immediately investigate and provide timely notification to affected persons, to HHS, and to the media, 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.

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).

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.

Step 23: Complaints

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.

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.

Step 24: Fundraising

Policy

Our dental practice will obtain appropriate patient authorization when required before using or disclosing patient information for fundraising purposes.

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.

Step 25: Review and Revise

Policy

Our dental practice will revise our HIPAA policies and procedures as necessary and appropriate to remain in compliance with HIPAA.

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 the current policies and procedures.

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).