Rabeni Dental

HIPAA Policies and Procedures

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.

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.

See additional list of Rabeni Dental Policies and Procedures that are specific to this practice.

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.

Step 4: 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.

Step 5: 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.

Step 6: 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.

Step 7: 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.

Step 8: 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.

Step 9: 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.

Step 10: 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.

Step 11: 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.

Step 12: 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.

Step 13: 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.

Step 14.1: 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.

Step 14.2: 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.

Step 14.3: 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.

Step 14.4: 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.

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.

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.

First violation: Privacy Official provides a verbal reminder.

Second violation: Reminder and workforce member required to participate in training.

Third violation: Reminder placed in employee's personnel file with warning that repeat offense will result in time off without pay; additional retraining.

Fourth violation: Suspension for three (3) days without pay.

Fifth violation: Workforce member employment terminated.

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.

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.

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 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.

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:

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.

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.

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 a 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.

All paper documents containing PHI that need to be disposed of will be placed in the shredder.

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.

Technical Safeguard Procedures:

[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.

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.

Workforce member will change the view of the appointment schedule to only show procedures to be done without any patient names.

Each workforce member has a unique username and password to log in to each computer work station.

After a couple minutes of inactivity, the computer monitor will lock and the user will need to login again with username and password.

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.

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 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.

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.

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.

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.