2.1.2.1 Consistent with Notice of Privacy Practices

Policy
Our practice will not disclose without patient authorization protected health information in a manner that is inconsistent with our NPP or state law.
Procedures
Any requests to obtain protected health information will be directed to our Privacy Officials who then will verify whether the use or disclosure is consistent with our Notice of Privacy Practices and state and federal laws.
In areas where state and federal law are inconsistent, our practice will consult legal counsel.

2.1.2.2 Consistent with other Documents

Policy
Our Privacy and Security Officials will collaborate to ensure security requirements, state laws, and privacy safeguards are consistent with our privacy policies and procedures.

Procedures
Our Privacy and Security Officials will review Privacy, Security, Patient Identity Protection, Breach Notification, Business Associate Agreement, health plan contract, and other applicable documents to ensure continuity and consistency regarding our practice's protected health information use and disclosure policies and procedures.

2.1.3 Policies and Procedures

Policy
Our practice will implement policies and procedures that are designed to comply with the HIPAA Privacy Rule and the Breach Notification Rule. At the same time, our policies and procedures will comply with applicable state laws.
Procedures
Our Privacy Officials are responsible for developing and updating our privacy policies and procedures.

Under the Privacy Officials' direction, our practice will review each of the Standards identified in the HIPAA Privacy and Breach Notification Rules, determine how we will comply with each Standard, develop policies and procedures that meet the requirements, and document them.

All members of our workforce will have access to our policies and procedures either electronically or on paper. An additional copy will be placed in our library.

As liability can now be extended to employers and individuals, each workforce member will receive a copy of our updated policies and procedures and sign an acknowledgement form[1] that he or she understands the policies and procedures, and will comply with them. Such forms shall be retained according to the HIPAA documentation Standard.

---

[1] See Appendix 2-5 for sample form: *Acknowledgement of Receipt of HIPAA Privacy Policies and Procedures.*

If a patient requests records:

1. Photo ID
2. What info is being requested?
3. Obtain a release form signed by patient and put in chart.
4. Provide requested information, collect fee if applicable.
5. Document on chart that information what given to patient.

If a patient's representative requests information:

1. Evaluate relationship between patient and representative. Consult with privacy officials if necessary.
2. Photo ID
3. Obtain a release form signed by representative and patient if possible and put in chart.
4. Document in chart the person's request to obtain the information and also document why information was or was not divulged to the person requesting it.

A personal representative[2] is legally responsible for the individual's care and general condition. A personal representative can be named in accordance with state or federal law. For example, the personal representative of a minor child is usually the child's parent or legal guardian.

In the case of a custody decree, the personal representative is the parent who can make health care decisions for the child under the decree. If you do not know the patient or parent, you should ask to see a copy of the divorce decree and a photo ID.

The personal representative may also present documentation including a health care power of attorney. Make a copy of this document and include it in the patient's health record. When an individual dies, the personal representative for the deceased is the executor or administrator of the deceased individual's estate, or the person who is legally authorized by a court or by state law to act on behalf of the deceased individual or the estate.

If you reasonably believe the personal representative might endanger the patient, such as in cases of domestic violence, abuse, or neglect, you can refuse to provide protected health information. Be sure to document your decision. If you suspect the patient is a victim of abuse, neglect, or domestic violence, you may as a Covered Entity disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.[3]

If the person requesting protected health information is…	**Then**
The patient appearing in person	Request a photo ID and one other piece of information that is on the medical record, such as address, social security number, or date of birth for verification.
The patient, but on the phone	If you do not recognize the person's voice, ask for several pieces of information to help identify the individual. This may include last name, date of birth, address, or approximate date last seen in our practice.
A friend or family member	Request a photo ID; require signature from the person requesting protected health information. When identity has

[2] Consult the Office for Civil Rights for more details on what is a Personal Representative. http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/personalreps.html.
[3] 45 CFR 164.512(a), (b)(1)(ii), and (c).

	been verified, see Section 2.2.4 regarding disclosures to friends or family members (pp.18-19).
A personal representative	If a personal representative accompanies the individual, exercise professional judgment to verify that this person is acting on behalf of the individual and verify his or her identity. If you are unsure of the representative, request a copy of the Power of Attorney or other document, such as for verifying legal guardianship; and request a photo ID. When identity has been verified, see Section 2.2.1 regarding disclosures to personal representatives (pp. 14-15).
A public official	Request to see the identification badge or other official credentials; or if the request is in writing, review the appropriate government letterhead, insignia, address, and credentials. When identity has been verified, see Section 2.2.6, "Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is not Required," for more information regarding permissible disclosures to public officials (pp. 21-25).

Sign-In sheets:
LAST NAME ONLY and time of arrival on the sign in sheet.

Information that is considered Personal Health Information:

- Names
- All geographic info smaller than state
- Dates (except year)
- Phone numbers
- Photos
- Fax numbers
- Email address
- SSN
- License #
- Medical Record #
- Insurance ID #

* Remember: Do not volunteer the information we have on file when verifying the patient's identity, the patient should be able to provide you with this information.*

2.5 HIPAA Privacy Safeguards

Policy
Our dental practice will exercise care to safeguard the use and disclosure of protected health information. The following procedures identify how we will safeguard protected health information in oral, hard copy (paper and other physical documentation such as dental films), and electronic formats.

1.5.1 Administrative Safeguard Procedures:

Sign-in Sheets: Patients will sign in using last name only and time of arrival. Dental staff will call patients by first name into the exam room.

Oral communications: Our workforce members will avoid unnecessary disclosures of protected health information by monitoring their voice levels and being alert for unauthorized listeners. Dictation and telephone conversations will be conducted away from public areas. Speaker-phones may be used only in private areas.

Telephone messages: Unless a patient has requested that he or she be contacted specifically by alternative means of communication,[4] telephone messages and appointment reminders may be left on answering machines and voicemail systems, but we shall limit the amount of protected health information disclosed in a telephone message. If we suspect abuse or neglect, we will seek an alternative means of communication for messages.

Faxes: Only the protected health information necessary to meet details of the request will be faxed. A cover sheet that includes a confidentiality notice will accompany all faxes. We will make reasonable efforts to verify that a fax transmission was sent to the correct destination.

Fax machines will be located in secure areas that cannot be easily accessed by visitors or patients.

Misdirected faxes containing protected health information must be accounted for in our Accounting of Disclosures Log. Any misdirected fax must be investigated and assessed under the Breach Notification Rule; if the misdirected fax constitutes a breach of unsecured protected health information, appropriate notifications will be sent.

Mail: Protected health information that is mailed will be concealed and sent via first class mail to the patient's primary address unless the patient requests an alternative address.

Copies: Copies of records containing protected health information will be stamped "Copy" in a color other than black so that copies can be distinguished from originals.

---

[4] See Section 2.4.4, pp. 48-49, "Confidential Communications Requirements."