
Dakota Smiles Mobile Dental Program

SITE PARTNER HEALTH INFORMATION PRIVACY POLICIES & PROCEDURES

These Health Information Privacy Policies & Procedures implement our obligations to protect the privacy of individually identifiable health information that we create, receive, or maintain as a healthcare provider.

We implement these Health Information Privacy Policies and Procedures as a matter of sound business practice; to protect the interests of our patients; and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), its implementing regulations at 45 CFR Parts 160 and 164 (65 Fed. Reg 82462 (Dec. 28, 2000)) (“Privacy Rules”), as amended (67 Fed. Reg. 53182 [Aug. 14, 2002]), and state law that provides greater protection or rights to patients than the Privacy Rules.

As a member of our workforce or as our Business Associate, you are obligated to follow these Health Information Privacy Policies & Procedures faithfully. Failure to do so can result in disciplinary action, including termination of your employment or affiliation with us.

These Policies & Procedures address the basics of HIPAA and the Privacy Rules that apply in our dental practice. They do not attempt to cover everything in the Privacy Rules. The Policies & Procedures sometimes refer to forms we use to help implement the policies and to the Privacy Rules themselves when added detail may be needed.

Please note that while the Privacy Rules speak in terms of “individual” rights and actions, these Policies & Procedures use the more familiar word “patient” instead; “patient” should be read broadly to include prospective patients, patients of record, former patients, their authorized representatives, and any other “individuals” contemplated in the Privacy Rules.

If you have questions or doubts about any use or disclosure of individually identifiable health information or about your other obligations under these Health Information Privacy Policies & Procedures, the Privacy Rules or other federal or state law, consult the Privacy Officer at 605-224-7345 , before you act.

The Dakota Smiles Mobile Dental Program

Adopted Effective: 5/17/2004

1. General Rule: No Use or Disclosure

The Care Unit must not use or **disclose protected health information (PHI)**, except as these Privacy Policies & Procedures permit or require.

2. Acknowledgement

The Care Unit will make a good faith effort to obtain a written acknowledgement of receipt of our **Notice of Privacy Practices** (see Section 9) from a patient before we use or disclose his or her protected health information (PHI) for treatment, to obtain payment for that treatment, or for our healthcare operations (TPO).

The Care Unit's use or disclosure of PHI for our payment activities and healthcare operations may be subject to the minimum necessary requirements (see Section 7).

3. Authorization

In some cases we must have proper, written **Authorization** from the patient (or the patient's personal representative) before we use or disclose a patient's PHI for any purpose (except for TPO purposes) or as permitted or required without consent or authorization (see Sections 3, 4, or 5).

The Care Unit will use the **Authorization** form. We will always act in strict accordance with an **Authorization**.

a) Authorization Revocation – A patient may revoke an authorization at any time by written notice. Our dental office will not rely on an **Authorization** we know has been revoked.

b) Authorization from Another Provider – The Care Unit will use or disclose PHI as permitted by a valid **Authorization** we receive from another healthcare provider.

The Care Unit may rely on that covered entity to have requested only the minimum necessary protected PHI. Therefore, the Care Unit will not make our own "minimum necessary" determination, unless we know that the **Authorization** is incomplete, contains false information, has been revoked, or has expired.

c) Authorization Expiration – The Care Unit will not rely on an **Authorization** we know has expired.

4. Oral Agreement

The Care Unit may use or disclose a patient's PHI with the patient's **Oral Agreement** or if the patient is unavailable subject to all applicable requirements.

The Care Unit may use professional judgment and our experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the patient to pick up dental/medical supplies, X-rays, or other similar forms of PHI.

5. Permitted Without Acknowledgement, Consent Authorization or Oral Agreement

The Care Unit may use or disclose a patient's PHI in certain situations, without **Authorization** or **Oral Agreement**. In the Care Unit, these disclosures are not likely to be frequent.

a) Verification of Identity – The Care Unit will always verify the identity of any patient, and the identity and authority of any patient's personal representative, government or law enforcement official, or other person, unknown to us, who requests PHI before we will disclose the PHI to that person.

The Care Unit will obtain appropriate identification and, if the person is not the patient, evidence of authority. Examples of appropriate identification include photographic identification card, government identification card or badge, and appropriate document on government letterhead. The Care Unit will document the incident and how we responded.

b) Uses or Disclosures Permitted under this Section 5 – The situations in which the Care Unit is permitted to use or disclose PHI in accordance with the procedures set out in this Section 5 are listed below.

- May disclose a patient’s PHI to that patient on request.
- May disclose to a patient’s personal representative PHI relevant to the representative capacity. We will not disclose to a personal representative we reasonably believe may be abusive to a patient any PHI we reasonably believe may promote or further such abuse.
- Will not use or disclose a patient’s PHI for fundraising purposes without the patient’s **Authorization**.
- Will not use or disclose PHI for marketing without a patient’s **Authorization** unless the marketing is in the form of a promotional gift of nominal value that we provide, or face-to-face communications between us and the patient.
- May use or disclose PHI in the following types of situations, provided procedures specified in the Privacy Rules are followed:
 1. For public health activities;
 2. To health oversight agencies;
 3. To coroners, medical examiners, and funeral directors;
 4. To employers regarding work-related illness or injury;
 5. To the military;
 6. To federal officials for lawful intelligence, counterintelligence, and national security activities;
 7. To correctional institutions regarding inmates;
 8. In response to subpoenas and other lawful judicial processes;
 9. To law enforcement officials;
 10. To report abuse, neglect, or domestic violence;
 11. As required by law;
 12. As part of research projects; and
 13. As authorized by state worker’s compensation laws.

6. Required Disclosures

The Care Unit will disclose protected health information (PHI) to a patient (or to the patient’s personal representative) to the extent that the patient has a right of access to the PHI (see Section 10); and to the U.S. Department of Health and Human Services (HHS) on request for complaint investigation or compliance review.

The Care Unit will use the disclosure log to document each disclosure we make to HHS.

7. Minimum Necessary

The Care Unit will make reasonable efforts to disclose, or request of another covered entity, only the **minimum necessary** protected health information (PHI) to accomplish the intended purpose.

There is **no minimum necessary** requirement for disclosures to or requests by one another in our dental office or by a healthcare provider for treatment; permitted or required disclosures to, or for disclosure requested and authorized by, a patient; disclosures to HHS for compliance reviews or complaint investigations; disclosures required by law; or uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules.

a) Routine or Recurring Requests or Disclosures – The Care Unit will follow the policies and procedures that we adopt to limit our routine or recurring requests for our disclosures of PHI to the minimum reasonably necessary for the purpose.

b) Non-Routine or Non-Recurring Requests or Disclosures – No non-routine or non-recurring request for or disclosure of PHI will be made until it has been reviewed on a patient-by-patient basis against our criteria to ensure that only the minimum necessary PHI for the purpose is requested or disclosed.

c) Other's Requests – The Care Unit will rely, if reasonable for the situation, on a request to disclose PHI being for the minimum necessary, if the requester is: (a) a covered entity; (b) a professional (including an attorney or accountant) who provides professional services to our practice, either as a member of our workforce or as our **Business Associate**, and who represents that the requested information is the minimum necessary; (c) a public official who represents that the information requested is the minimum necessary; or (d) a researcher presenting appropriate documentation or making appropriate representations that the research satisfies the applicable requirements of the Privacy Rules.

d) Entire Record – The Care Unit will not use, disclose, or request an entire record, except as permitted in these Policies & Procedures or standard protocols that we adopt reflecting situations when it is necessary.

e) Minimum Necessary Workforce Use – The Care Unit will use only the minimum necessary PHI needed to perform our duties.

8. Business Associates

The Care Unit will obtain satisfactory assurance in the form of a written contract that our **Business Associates** will appropriately safeguard and limit their use and disclosure of the protected health information (PHI) we disclose to them.

These **Business Associate** requirements are not applicable to our disclosures to a healthcare provider for treatment purposes. The **Business Associate Contract Terms** document contains the terms that federal law requires be included in each **Business Associate Contract**.

a) Breach by Business Associate – If the Care Unit learns that a **Business Associate** has materially breached or violated its **Business Associate Contract** with us, we will take prompt, reasonable steps to see that the breach or violation is cured.

If the **Business Associate** does not promptly and effectively cure the breach or violation, we will terminate our contract with the **Business Associate**, or if contract termination is not feasible, report the **Business Associate's** breach or violation to the U.S. Department of Health and Human Services (HHS).

9. Notice of Privacy Practices

The Care Unit will maintain a **Notice of Privacy Practices** as required by the Privacy Rules.

a) Our Notice – We will use and disclose PHI only in conformance with the contents of our **Notice of Privacy Practices**. We will promptly revise a **Notice of Privacy Practices** whenever there is a material change to our uses or disclosures of PHI to legal duties, to the patients' rights or to other privacy practices that render the statements in that Notice no longer accurate.

b) Distribution of Our Notice – We will provide our **Notice of Privacy Practices** to any person who requests it, and to each patient no later than the date of our first service delivery after May 17, 2004.

We will have our **Notice of Privacy Practices** available for patients to take with them. We will also post our **Notice of Privacy Practices** in a clear and prominent location where it is reasonable to expect patients seeking services from us will be able to read the Notice.

c) Acknowledgement of Notice – We will make a good faith effort to obtain from the patient a written Acknowledgement of receipt of our **Notice of Privacy Practices**.

We shall use, **Acknowledgement of Receipt of Notice of Privacy Practices** to obtain the Acknowledgement. If we cannot obtain written Acknowledgement from the patient, we will use the form to document our attempt and the reason why written Acknowledgement was not signed by the patient.

10. Patients' Rights

We will honor the rights of patients regarding their PHI.

a) Access – With rare exceptions, we must permit patients to request access to the PHI we or our **Business Associates** hold.

No PHI will be withheld from a patient seeking access unless we confirm that the information may be withheld according to the Privacy Rules. We may offer to provide a summary of the information in the chart. The patient must agree in advance to receive a summary and to any fee we will charge for providing the summary. We will contact our **Business Associates** to retrieve any PHI they may have on the patient.

b) Amendment – Patients have the right to request to amend their PHI and other records for as long as our the Care Unit maintains them.

We may deny a request to amend PHI or records if: (a) we did not create the information (unless the patient provides us a reasonable basis to believe that the originator is not available to act on a request to amend); (b) we believe the information is accurate and complete; or (c) we do not have the information.

We will follow all procedures required by the Privacy Rules for denial or approval of amendment requests. We will not, however, physically alter or delete existing notes in a patient's chart. We will inform the patient when we agree to make an amendment, and we will contact our **Business Associates** to help assure that any PHI they have on the patient is appropriately amended. We will contact any individuals whom the patient requests we alert to any amendment to the patient's PHI. We will also contact any individuals or entities of which we are aware that we have sent erroneous or incomplete information and who may have acted on the erroneous or incomplete information to the detriment of the patient.

When we deny a request for an amendment, we will mark any future disclosures of the contested information in a way acknowledging the contest.

c) Disclosure Accounting – Patients have the right to an accounting of certain disclosures our the Care Unit made of their PHI within the 6 years prior to their request. Each disclosure we make, that is not for treatment payment or healthcare operations, must be documented showing the date of the disclosure, what was disclosed, the purpose of the disclosure, and the name and (if known) address of each person or entity to whom the disclosure was made. The **Authorization** or other documentation must be included in the patient's record. We use the patient's chart to track each disclosure of PHI as needed to enable us to fulfill our obligation to account for these disclosures.

We are not required to account for disclosures we made: (a) before May 17, 2004; (b) to the patient (or the patient's personal representative); (c) to or for notification of persons involved in a patient's healthcare or payment for healthcare; (d) for treatment, payment, or healthcare operations; (e) for national security or intelligence purposes; (f) to correctional institutions or law enforcement officials regarding inmates; or (g) according to an Authorization signed by the patient or the patient's representative; (h) incident to another permitted or required use disclosure.

We will temporarily suspend the accounting of any disclosure when requested to do so pursuant according to the Privacy Rules by health oversight agencies or law enforcement officials. We may charge for any accounting that is more frequent than every 12 months, provided the patient is informed of the fee before the accounting is provided. We will contact our **Business Associates** to assure we include in the accounting any disclosures made by them for which we must account.

d) Restriction on Use or Disclosure – Patients have the right to request the Care Unit to restrict use or disclosure of their PHI, including for treatment, payment, or healthcare operations. We have no obligation to agree to the request, but if we do, we will comply with our agreement (except in an appropriate dental/medical emergency).

We may terminate an agreement restricting use or disclosure of PHI by a written notice of termination to the patient. We will contact our **Business Associates** whenever we agree to such a restriction to inform the **Business Associate** of the restriction and its obligations to abide by the restriction. We will document in the patient's chart any such agreed to restrictions.

e) Alternative Communications – Patients have the right to request us to use alternative means or alternative locations when communicating PHI to them. Our dental office will accommodate a patient's request for such alternative communications if the request is reasonable and in writing.

Our dental office will inform the patient of our decision to accommodate or deny such a request. If we agree to such a request, we will inform our Business Associates of the agreement and provide them with the information necessary to comply with the agreement.

f) Applicability – The Care Unit will be aware of and respect these patients' rights regarding their PHI, even though in most situations patients are unlikely to exercise them.

11. Staff Training and Management, Complaint Procedures, Data Safeguards, Administrative Practices

a) Staff Training and Management

* **Training** – The Care Unit will train all members of our workforce in these Privacy Policies & Procedures, as necessary and appropriate for them to carry out their functions.

The Care Unit will train each new staff member within a reasonable time after the member starts. We will also retrain each staff member whose functions are affected either by a material change in our Privacy Policies and Procedures or in the member's job functions, within a reasonable time after the change.

***Discipline and Mitigation** – The Care Unit will develop, document, disseminate, and implement appropriate discipline policies for staff members who violate our Privacy Policies & Procedures, the Privacy Rules, or other applicable federal or state privacy law.

Staff members who violate our Privacy Policies & Procedures, the Privacy Rules or other applicable federal or state privacy law will be subject to disciplinary action, possibly up to and including termination of employment.

b) Complaints – The Care Unit will implement procedures for patients to complain about our compliance with our Privacy Policies and Procedures or the Privacy Rules. We will also implement procedures to investigate and resolve such complaints.

c) Data Safeguards – The Care Unit will “add to” and strengthen these Privacy Policies & Procedures with such additional data security policies and procedures as are needed to have reasonable and appropriate administrative, technical, and physical safeguards in place to ensure the integrity and confidentiality of the PHI we maintain.

The Care Unit will take reasonable steps to limit incidental uses and disclosures of PHI made according to an otherwise permitted or required use or disclosure.

d) Documentation and Record Retention – The Care Unit will maintain in written or electronic form all documentation required by the Privacy Rules for six years from the date of creation or when the document was last in effect, whichever is greater.

12. State Law Compliance

The Care Unit will comply with the privacy laws of each state that has jurisdiction over our practice, or its actions involving protected health information (PHI), that provide greater protections or rights to patients than the Privacy Rules.

13. HHS Enforcement

The Care Unit will give the U.S. Department of Health and Human Services (HHS) access to our facilities, books, records, accounts, and other information sources (including individually identifiable health information without patient authorization or notice) during normal business hours (or at other times without notice if HHS presents appropriate lawful administrative or judicial process).

We will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of our practice.

14. Designated Personnel

We will designate a Privacy Officer and other responsible persons as required by the Privacy Rules.