Smile Valley Pediatric Dentistry
4910 Massachusetts Avenue #311
Washington, DC 20016
202-237-2833

HIPAA NOTICE OF PRIVACY PRACTICES

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

The confidentiality of your personal health information is very important to us. Your health information includes records that we create and obtain when we provide you care, such as a record of your symptoms, examination and test results, diagnoses, treatments and referrals for further care. It also includes bills, insurance claims, or other payment information that we maintain related to your care. After reviewing this Notice, if you need further information or want to contact us for any reason regarding the handling of your dental health information, please direct any communications to the above entity.

We are required by law to:

- Maintain the privacy of protected health information as required by law.
- Give you this notice of our legal duties and privacy practices regarding your health information.
- Follow the terms of the Notice currently in effect.

How we may use and disclose your health information:
The following are ways we may use and disclose your protected health information. Except for the purposes listed in this Notice or other limited purposes specifically permitted by applicable law, such as certain disclosures for law enforcement or national security purposes, we will use and disclose your health information only with your authorization.

Treatment
We may use and disclose your health information for treatment and to provide you with treatment-related health care services. We may also share your health information with other healthcare providers, agencies or facilities involved in your care in order to provide or coordinate the different treatments you need, such as prescriptions or other types of dental treatment. We also may disclose health information about you to people who may be involved in your continuing care after you leave our practice.

Payment
We may use and disclose your health information so that we may bill and receive payment from you, an insurance company, or a third party for the treatment and services you received. For example, we may inform your insurance company that you received a certain type of treatment so that we might receive payment for providing that treatment.

Health Care Operations
We may use and disclose your health information for purposes relating to the proper

operation of our practice, including to evaluate and improve our dental care and to operate and manage our office. For example, we may use and disclose information to a peer review organization or a health plan that is evaluating our care. We may use your health information to contact you about services that are available from us. We may also share information with other health care providers that have a relationship with you for their treatment, payment or health care operations activities.

Appointment Reminders, Treatment Alternatives, and Health-Related Benefits and Services

We may use and disclose your health information to contact you and remind you of your appointment, to tell you about treatment alternatives or health-related benefits and services you could use.

Minors

If you are an unemancipated minor under District of Columbia law, there may be circumstances in which we disclose health information about you to a parent, guardian, or other person acting *in loco parentis,* in accordance with our legal and ethical responsibilities.

Disaster Relief

We may disclose health information about you to government entities or private organizations (such as the Red Cross) to assist in disaster relief efforts. If you are available, we will provide you an opportunity to object before disclosing any such information. If you are unavailable because, for example, you are incapacitated, we will use our professional judgment to determine whether disclosure is in your best interest and is necessary to ensure an adequate response to the emergency circumstances.

As Required by Law

We will disclose your health information when required to do so by law or by applicable legal process, such as disclosures in lawsuits in which we are a party or when we are served with legal process such as a subpoena in a lawsuit in which we are not a party.

Business Associates

We may disclose your health information to our business associates that perform functions on our behalf or provide us with professional services. For example, we may use another company to perform billing services on our behalf. All of our business associates are obligated to protect the privacy of your health information.

Public Health Disclosures

We may disclose your health information for public health purposes. These purposes generally include the following: (1) preventing or controlling disease (such as cancer and tuberculosis), injury or disability; (2) reporting vital events such as births and deaths; (3) reporting child abuse or neglect; (4) reporting adverse events or surveillance related to food, medications or defects; (5) reporting problems with products; (6) notifying a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; (7) notifying the appropriate government authority if we believe a patient has been the victim of abuse or neglect and make this disclosure as authorized or required by law; (8) notifying the coroner of a patient's death; (9) notifying emergency response employees regarding possible exposure to HIV/AIDS, to the extent necessary to comply with state and federal law; (1) notifying multidisciplinary personnel teams relevant to the prevention,

identification, management, or treatment of an abused child and the child's parents or an abused elder or dependent adult

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

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

Law Enforcement
We may release, as appropriate, your health information to law enforcement: (1) pursuant to a subpoena by law enforcement; (2) as needed for the protection of others; or (3) if there is a court order, subpoena, or other legal process for release of the information.

Safeguarding Protected Health Information

This office will implement appropriate safeguards to protect PHI whether in written, oral, or electronic format to reduce the likelihood of an inappropriate or unauthorized use or disclosure.

Verbal Communication

- Workers must be aware of their surroundings when having conversations involving PHI.
- Discuss issues in a secure location (e.g. patient room or office), especially when discussing communicable diseases, mental health, substance abuse, or financial issues.
- Discuss patient information only with other workers who are involved in that patient's care. Dictation and telephone conversations should occur away from public areas whenever possible.
- When leaving telephone voice messages or appointment reminders, only leave the minimum necessary information.

Training

- All workers, including temporary employees, volunteers, interns, and students, will be trained on the HIPAA Privacy and Security Rules. This training will occur within a reasonable period of time after a new member joins the workforce and annually thereafter.
- This training will include a review of the pertinent regulations, definition of breach, and safeguards to protect patient information.

- Training documentation will be kept for a period of no less than six (6) years by the Privacy Officer or Office Manager.

Patients and Visitors

- Patients will be accompanied to the patient care area.
- Visitors will only be allowed access to approved areas of this office. Visitors include service providers (e.g. shredding, package delivery), manufacturer representatives, and repair personnel.
- Movement within the office will be monitored to reduce the likelihood of unauthorized access to PHI.

Disposal of Protected Health Information

- Any media containing PHI should only be discarded in the appropriately identified and secured container.
- Paper copies of PHI waiting to be shredded (e.g. after data entry) should be promptly placed in a secure storage container/area before shredding occurs.
- Electronic media will be destroyed according to procedures in the Disposal of Media Containing PHI in the Security Plan of this Manual.

Computers

- Computers will be positioned so that PHI cannot be viewed by unauthorized personnel or visitors. If necessary, a privacy filter will be used on the computer monitor.
- Workers will log off or lock their computers when left unattended.
- Computers are set to automatically log-out/lock after being idle for a short period of time.

Tablets/Laptops/Thumb Drives/Smartphones

- PHI should not be stored on portable devices unless a proper safeguard (e.g. encryption) is in place. Any unassigned portable devices will be signed out PRIOR to leaving this office.
- Additional safeguards for portable devices:
    - Do not leave unattended.
    - Enable screen lock passwords and remote wiping capabilities.
    - Immediately report the loss of portable device to the Privacy Officer or Office Manager.

Social Media

- Workers are not permitted to discuss PHI on any personal social media account, including just the patient's name.
- Workers should refrain from accessing personal social media accounts on network computers.

Emailing Protected Health Information

- Emails that contain PHI or have PHI in an attachment will occur in a secure manner. Attachments will be password protected.
- This office does not have a secure means of emailing patient information outside of this office.

- Limited information will be sent via unsecured email. Additional protections include:
    - If a patient requests this office to send PHI via email, the patient will be informed of the potential risks.
    - We honor this request once the patient has acknowledged the information will be sent in an unsecured manner.

Digital Copiers/Scanners/Fax

- After scanning paper containing PHI, paper will be placed in a secure place or shredded. The scanned file will be filed/uploaded to a secure location (e.g. EHR). Files containing PHI will not be kept on a computer's desktop.
- Security features will be enabled on digital copiers, scanners, and fax machines used by this office.

Mitigation

- This office will mitigate, to the extent possible, any harmful effect that we become aware of related to the unauthorized use or disclosure of PHI by this office or our Business Associate(s).

PATIENT ACKNOWLEDGMENT OF RECEIPT OF HIPAA NOTICE OF PRIVACY PRACTICES

Patient Name:_____
(maiden/other name used if applicable)

DOB:_____/_____/_____

I acknowledge that I have received a copy of the HIPAA Notice of Privacy Practices of Smile Valley Pediatric Dentistry effective January 1, 2023.

Parent Signature:_____

Date:_____/_____/_____