



NOTICE OF PRIVACY PRACTICES

Effective Date: 02/16//2026

This Notice describes how medical and dental information about you may be used and disclosed and how you can access this information. Please review it carefully.

OUR RESPONSIBILITIES

We are required by law to:

- Maintain the privacy and security of your protected health information (PHI).
- Provide you with this Notice of our legal duties and privacy practices.
- Abide by the terms of the Notice currently in effect.
- Notify you following a breach of unsecured PHI as required by federal and state law.

We reserve the right to change our privacy practices and the terms of this Notice at any time, consistent with applicable law. Any changes will apply to all PHI we maintain. The revised Notice will be available upon request, in our offices, and on our website.

Special Protection for Substance Use Disorder Records (If Applicable)

If we create or receive records related to substance use disorder (SUD) treatment, those records may receive additional federal protections under 42 CFR Part 2.

HOW WE MAY USE AND DISCLOSE YOUR INFORMATION

We may use and disclose your PHI for the following purposes without your authorization, as permitted by law:

Treatment: To provide, coordinate, or manage your dental care and related services.

Payment: To bill and collect payment for services provided, including disclosures to insurers or other payors.

Health Care Operations: For administrative, operational, legal, compliance, quality assessment, training, and business management activities.

Appointment Reminders and Treatment Alternatives: To contact you regarding appointments, follow-up care, or treatment options.

Business Associates: To third parties who perform services on our behalf and are required by contract to protect your PHI.

Family Members and Others Involved in Your Care: When you agree, when you are given the opportunity to object and do not, or when permitted by law based on professional judgment.

As Required by Law: For public health reporting, abuse or neglect reporting, law enforcement requests, judicial or administrative proceedings, and other legal requirements.

Breach Notification: To notify you and appropriate authorities of a breach of unsecured PHI as required by law.

Fundraising Communications: You may receive limited fundraising communications. You have the right to opt out of such communications at any time.

We will not use or disclose your PHI for marketing purposes or sell your PHI without your written authorization, except as permitted by law.

YOUR RIGHTS

You have the right to:

- Access and obtain a copy of your medical and dental records.
- Request corrections or amendments to your records.
- Request restrictions on certain uses or disclosures.
- Request confidential communications.
- Receive an accounting of certain disclosures.
- Obtain a paper or electronic copy of this Notice.
- File a complaint without retaliation.

All requests must be submitted in writing. Reasonable, cost-based fees may apply for copies as permitted by law.

CONTACT INFORMATION

If you have questions, concerns, or wish to exercise your rights, please contact:

Privacy Officer
Emergency Dental of America
4611 S. 96th Street
Omaha, NE 68127
Email: jmlynarik@emergencydentalusa.com

You may also file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights.

ACKNOWLEDGMENT OF RECEIPT

I acknowledge that I have received a copy of the Notice of Privacy Practices.

Signature: _____ Date: _____

Printed Name: _____

Relationship to Patient (if applicable): _____

STATE-SPECIFIC PRIVACY NOTICE

Certain states provide additional privacy rights or impose stricter requirements than federal HIPAA regulations, including but not limited to laws governing mental health records, HIV/AIDS information, genetic testing data, minors' records, breach notification timelines, and consumer privacy rights.

Where state or local law provides greater privacy protections than federal law, we comply with the more stringent requirement. Patients may request additional information regarding state-specific rights by contacting our Privacy Officer.

This Notice is intended to comply with applicable federal requirements (including HIPAA and HITECH), state privacy laws, dental board regulations, OSHA, and CDC guidance as in effect on January 1, 2026.

STATE-SPECIFIC PRIVACY ADDENDA

Effective Date: 01/01/2026

This addendum supplements the Emergency Dental of America Notice of Privacy Practices and applies only where state law provides greater privacy protections than federal HIPAA regulations. Where applicable, the stricter law governs.

CALIFORNIA (CA)

In addition to HIPAA, California law provides enhanced privacy protections under the Confidentiality of Medical Information Act (CMIA) and the California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA).

- Patient medical and dental information may not be disclosed without authorization except as permitted by law.
- Patients have rights to access, correction, limitation of use, and disclosure transparency.
- Emergency Dental of America does not sell or share patient information for cross-context behavioral advertising.
- Certain data breach notifications must occur within timelines shorter than federal HIPAA requirements.

COLORADO (CO)

Colorado law provides enhanced consumer and health data protections, including the Colorado Privacy Act.

- Patients have expanded rights related to access, correction, and data minimization.
- Breach notification must generally occur within 30 days of determination.
- Reasonable security safeguards are required for electronic PHI beyond HIPAA minimum standards.

FLORIDA (FL)

Florida law imposes stricter breach notification requirements and confidentiality standards.

- Breach notifications must generally be issued within 30 days.
 - Patient information must be protected using administrative, technical, and physical safeguards.
 - Certain disclosures require patient authorization even when HIPAA might permit disclosure.
-
-

NEW YORK (NY)

New York law provides enhanced privacy protections under state public health law and the SHIELD Act.

- Reasonable administrative, technical, and physical safeguards are required for PHI and private information.
 - Patients have enhanced protections for mental health, HIV/AIDS, genetic, and substance use treatment records.
 - Breach notifications may be required to state authorities and affected individuals.
-
-

TEXAS (TX)

Texas law provides some of the most stringent health information privacy requirements in the U.S.

- HIPAA privacy standards apply to a broader range of entities and data.
- Patient authorization is required for many disclosures otherwise permitted under HIPAA.
- Workforce members must receive privacy training at least every two years.
- Civil and criminal penalties may apply for improper disclosure.

Patients may contact the Privacy Officer for additional state-specific rights information.