NOTICE OF PRIVACY PRACTICES – This notice describes how medical information about you may be used and disclosed and how you can get access to this information. PLEASE REVIEW CAREFULLY.

This Notice is effective 02/10/2026 and replaces all earlier versions.

I. Our organization is committed to protecting health information about you. We create a record of the health care and service you receive at **Endodontic Associates** for use in your care and treatment. We need this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all the records of your care relating to services provided in the hospitals, outpatient and ambulatory care centers and other facilities that comprise the **Endodontic Associates**, as well as the physicians and other health care professionals who provide services within those entities. If your personal health care provider (provider) is not an employee of **Endodontic Associates**, then your provider may have different policies or Notices regarding how information maintained by the provider's office or clinic is used or disclosed about you.

We are required by law to:

- **Make sure that your health information is protected;**
- **Give you this Notice describing our legal duties to protect your privacy;**
- **Follow the terms of the Notice that is currently in effect; and**
- **Notify you in the event of a breach of your unsecured protected health information (PHI) as required by law.**

You have a right to receive a copy of and discuss this Notice with our Privacy Office at the number or address listed at the end of this Notice.

II. HOW WE MAY USE AND DISCLOSE PROTECTED HEALTH INFORMATION ABOUT YOU:

The following sections describe ways that an entity may use and disclose your protected health information. For each category of uses or disclosures, we will describe them and give some examples. Some information, such as genetic information, certain drug and alcohol information, HIV information and mental health information may be entitled to special restrictions by state and federal laws. We abide by all applicable state and federal laws related to the protection of this information. Not every use or disclosure will be listed; however, all the ways we are permitted to use and disclose information will fall within one of the following categories.

A. For Treatment - We may use protected health information about you to provide you with treatment or services. We may disclose your health information with other professionals involved in your care, agencies, or facilities not affiliated with **Endodontic Associates** to provide or coordinate the different things you need, such as prescriptions, lab work, and X-rays. We may disclose this information with people who are involved in taking care of you. We may contact you to provide appointment reminders, obtain patient registration information, information about treatment alternatives or other health-related benefits and services that may be of interest to you or to follow up on your care.

B. For Payment - We may use and disclose your protected health information for billing and payment activities of Endodontic Associates and others involved in your care, such as an ambulance company. For example, we may use and disclose information so that **Endodontic Associates** or others involved in your care can obtain payment form you, an insurance company or another third party. We may also tell your health insurance company about a treatment you need to obtain for prior approval or check if your insurance will pay for the treatment.

C. For Healthcare Operations - We may use and disclose your health information for our health care operations, which are various activities necessary to run our business, provide quality health care services and contact you when necessary. We may disclose your protected health information to medical or nursing students and other trainees for review and learning purposes

D. Health Information Exchange (HIE) We may participate in an electronic Health Information Exchange ("HIE") to facilitate the sharing of your protected health information for treatment purposes. An HIE is a network in which providers participate in exchanging patient information in order to facilitate health care.

E. Business Associates and Service Providers: We may disclose your protected health information with third parties referred to as "Business Associates". Business Associates provide various services to or for **Endodontic Associates.** Examples include billing services, transcription services and legal services. We ensure that all Business Associates and service providers, regardless of their location, are obligated to protect your PHI in accordance with U.S. and international laws, including the Health Insurance Portability and Accountability Act (HIPAA). These measures include implementing appropriate safeguards to protect the privacy and security of your information.

F. Required by *Law* – We will disclose protected health information about you when required to do so by federal, state, and/or local law. This includes, however, is not limited to, disclosures to mandated patient registries, including reporting adverse events with medical devices, food, or prescriptions drugs to the Food and Drug Administration. We may also disclose protected health information to health oversight agencies for activities authorized by law. This includes but is not limited to the U.S. Department of Health and Human Services, accrediting agencies, auditors, and public health activities when preventing disease, helping with product recalls and reporting adverse reactions to medications, reporting suspected abuse, neglect, or domestic violence. We may also disclose health information for law enforcement purposes as required by law or in response to a valid subpoena, summons, court order or similar purpose.

G. Research: We may use and disclose your protected health information for certain research purposes in compliance with the requirements of applicable. Federal and state laws. All research projects, however, are subject to a special approval process, which establishes protocols to ensure that your protected health information will continue to be protected, when required, we will obtain a written authorization from you prior to using or disclosing your protected health information for research.

H. Substance Use Disorder (SUD) Treatment Information: If we receive or maintain any information about you form a SUD treatment program that is covered by 42 CFR Part 2 (a "Part 2 Program") through a general written consent you provide to the Part 2 Program to use and disclose the SUD record for purposes of treatment, payment or health care operations, we may use and disclose your SUD records for treatment, payment or health care operations as described in this Notice. If we receive or maintain your SUD record through specific consent you provide us or another third party, we will use and disclose your SUD record only as expressly permitted by you in your written consent as provided to us.

In no event will we use or disclose your SUD record, or testimony that describes the information contained in your SUD record, in any civil, criminal, administrative or legislative proceedings by any Federal, State or local authority against you, unless authorized by your consent or court order (after you are notified of the court order).

I. Facility Directories (Hospital Inpatients only) - Unless you object, we will use and disclose in our facility directory your name, the location at which you are receiving care (for example: room number or emergency room) and your general condition. The directory information may be released to people who ask for your name so your family, friends and clergy may visit you in the hospital and generally know how you are doing.

J. Individuals Involved in Your Care or Payment for your care: Unless you tell us not to, we will disclose your health information with anyone involved in your health care, such as a friend, family member or any individual you identify. If you are unable to agree or object, for example, if you are not present or are unconscious, we may disclose protected health information as necessary if we determine that it is in your best interest based on our professional judgment. Additionally, we may disclose information about you to your legal representative.

K. Legal Proceedings, Lawsuits and Other Legal Actions: We may disclose protected health information about you to courts, attorneys, court employees and others when we receive a court order, subpoena, discovery request, warrant, summons or other lawful instructions. We may also disclose information about you to **Endodontic Associates** attorneys and/or attorneys working on **Endodontic Associates** behalf to defend ourselves against a lawsuit or action brought against us. We may disclose your protected health information to the police or other law enforcement officials to report or prevent a crime as otherwise required or permitted by law.

L. Fundraising Activities – We may contact you to raise funds and provide information about Endodontic Associates activities, including fundraising programs and events. You may request to "opt-out" of fundraising communications if you do not wish to be contacted. Please email your request to ***billing@sanmateoendo.com*** or call ***(650) 340-0225*** to leave a message identifying yourself and stating that you wish to opt out.

M. We may use and disclose your protected health information in the following special situations:

- **Disaster Relief -** We may use or disclose your health information with an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.
- **Coroners, Funeral Directors, and Organ Donation:** We may disclose health information about you with organ procurement organizations. We may also disclose health information with a coroner, medical examiner, or funeral director when an individual dies.
- **Workers' Compensation and Other Government requests:** We may use or disclose health information about you for workers' compensation claims
- **National Security and Intelligence Activities**
- **Military:** If you are a member of the armed forces, domestic (United States) or foreign; we may disclose protected health information about you to the military authorities as authorized or required by law.
- **Protective Services for the President of the United State and Others:** We may disclose protected health information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities as required by law.

N. Artificial Intelligence or AI: We may utilize AI technology to support operational decisions and recommendations about your treatment or care, including but not limited to documenting care, supporting clinical assessments, treatment recommendations, creating a care plan, and billing. AI technology may use your information to train and improve AI technology's functionality. AI technology partners (Business Associates) are required to keep your information confidential.

O. (If Applicable) Sharing Information within an OHCA: We maintain our Designated Record Set through the use of an electronic health record ("EHR"). Through this EHR, your medical information is combined with that of other health care providers or "Covered Entities" that participate in the EHR (each, a "Participating Covered Entity" and collectively, the "Participating Covered Entities"), such that each of our patients,

including you, have a single, longitudinal health record with respect to all services provided by the Participating Covered Entities. Through
the EHR, the Participating Covered Entities have formed one or more organized systems of health care in which the Participating Covered Entities participate in joint utilization review and/or quality assurance activities, and as such qualify to participate in Organized Health Care
Arrangement(s) ("OHCA(s)"). As OHCA participants, all Participating Covered Entities, including us, may use and disclose the protected
health information contained within the EHR for the Treatment, Payment and Health Care Operations purposes of each of the OHCA participants.

III. YOU HAVE THE RIGHT TO ACCESS YOUR PROTECTED HEALTH INFORMATION BY CONTACTING THE LOCATION WHERE YOU RECEIVED YOUR CARE OR BY CALLING THIS NUMBER AT THE END OF THIS NOTICE.

In addition to your rights as a patient, we also ask that you respect the rights of other patients by not discussing any information you may see or hear while receiving services in our facilities.

YOUR RIGHTS REGARDING PROTECTED HEALTH INFORMATION ABOUT YOU.

You have the following rights regarding protected health information we maintain about you:

A. **Right to Inspect and obtain an Electronic or Paper Copy of your Protected health Information** – With certain exceptions, you have the right to inspect and/or receive an electronic or paper copy of your protected health and billing records and other health information used by us to make decisions about your care. You may request that we send a copy of your protected health information to a third party. To inspect and/or receive a copy of your protected health records we request you submit a request in writing to your **Endodontic Associates** provider or the appropriate health information department. If you request a copy of your protected health records, we may charge you a reasonable cost-based fee for the cost of providing you with the copies. Under certain circumstances, we may deny your request to inspect or copy your records. If we deny your request, we will explain the reasons to you and in most cases, you may have the denial reviewed.

B. **Right to Request an Amendment -** You may request that we amend health information about you that you think is incorrect or incomplete. You may ask us to correct the information if the information is kept by or **Endodontic Associates** in your protected health and billing records. To request an amendment, your request must be submitted in writing to the **Endodontic Associates** Privacy Office and provide the reasons for the request. If we agree to your request, we will amend your record(s) and notify you of such. In certain circumstances, we cannot remove what was in the record(s), however we may add supplemental information to clarify. If we deny your request for an amendment, we will provide you with a written explanation of why we denied it and explain your rights.

C. **Right to an Accounting of Disclosures –** You have a right to receive a list of certain disclosures we have made of your protected health information in the six (6) years prior to the date of your request. To request an accounting of disclosures, you must submit your request in writing to the **Endodontic Associates** Privacy Office. You must state the time period for which you want to receive the accounting, which may not date back more than six years from the date of your request. The first accounting you receive in a 12-month period will be free. We may charge you for responding to additional requests in that same time period.

D. **Right to Request Restriction** – You have the right to request a restriction or limitation on the protected health information we use or disclose about you for treatment, payment or health care operations. You alone have the right to request a limit on the protected health information we disclose about you to someone who is involved in your care or the payment for your care, such as a family member or friend. If we agree to your request, we will comply with your request unless the information is needed to

provide you with emergency treatment, or we are required by law to disclose it. We are not required to agree to your request except in the case where the disclosure is to a health plan for purposes of carrying out payment or health care operations of the health plan, and the information pertains solely to a protected health item or service for which you have paid out-of-pocket in full. To request a restriction, you must make your request to the **Endodontic Associates** Privacy Office and tell us (1) what information you want to limit, (2) whether you want to limit our use, disclosure, or both and (3) to whom you want the limits to apply, i.e. disclosures to your spouse. We are allowed to end the restriction if we tell you. If we end the restriction, it will only affect the protected health information that was created or received after we notify you.

E. **Right to a Paper Copy of This Notice** – You have the right to have a paper copy of this notice at any time, even if you have previously agreed to receive a copy of this Notice electronically. Copies of this Notice are available at **Endodontic Associates** facilities, on our website, **www.sanmateoendo.com** or by contacting the **Endodontic Associates** Privacy Office as shown below.

F. **Right to Choose Someone to Act for You** – If you have given someone healthcare power of attorney or if someone is your legal guardian, that person may exercise your rights and make choices about your health information. We will verify that the person has this authority and can act for you before we take action or disclose information.

IV. Uses of Medical Information Requiring Authorization

A. **Psychotherapy Notes** - We must obtain your written permission to disclose psychotherapy notes except in certain circumstances. For example, written permission is not required for use of those notes by the author of the notes with respect to your treatment or use or disclosure by us for training of mental health practitioners, or to defend **Endodontic Associates** in a legal action brought by you.

B. **Marketing** - We must obtain your written permission to use or disclose your medical information for marketing purposes except in certain circumstances. For example, written permission is not required for face-to-face encounters involving marketing, or where we are providing a gift of nominal value (example: a coffee mug), or a communication about our own services or products (example: we may send you a postcard announcing the arrival of a new surgeon or x-ray machine). Messaging opt-in consent will not be shared or sold for marketing purposes.

C. **Sale of Medical Information** - We must obtain your written permission to disclose your medical information in exchange for remuneration.

D. **Other Uses and Disclosures** - Other uses and disclosures of your medical information not covered by the categories included in this Notice or applicable laws, rules or regulations will be made only with your written permission or authorization. If you provide us with such written permission, you may revoke it at any time. We are not able to take back any uses or disclosures that we already made with your authorization. We are required to retain your medical information regarding the care and treatment that we provide to you.

V. CHANGES TO THIS NOTICE - We reserve the right to change this Notice and Endodontic Associates **privacy practices. We reserve the right to make the revised or changed Notice effective for protected health information we already have about you as well as any information we receive in the future. The new notice will be available upon request and on our web site. This Notice will specify the effective date of this Notice.**

VI. QUESTIONS/COMPLAINTS - If you believe your privacy rights have been violated, you may file a complaint with Endodontic Associates or with Endodontic Associates Privacy Officer. You will not be retaliated against for filing a complaint.

Marnie Burse
Endodontic Associates
(650) 340-0225
billing@sanmateoendo.com
235 N. San Mateo Dr., Ste. 400
San Mateo, Ca 94401

Or with **the Secretary of the Department of Health and Human Services:**

U.S. Dept. of Health and Human Services
Office for Civil Rights
2000 Independence Avenue, S.W.
Washington, D.C. 20201
1-877-696-6775

E-mail, Texting and Internet Use Policy

A. Coverage

Endodontic Associates (hereafter referred to as the 'Organization') workforce members, contract workers, temporary agency workers, business partners, and vendors) that access, use or disclose confidential patient and/or company information.

B. Reviewed/Revised

February 11, 2026

C. Purpose

The HIPAA Security Rule specifies that covered entities must "implement technical security measures to guard against unauthorized access to e-PHI that is being transmitted over an electronic communications network.", and "implement procedures to verify that a person or entity seeking access to ePHI is the one claimed." The purpose of this policy is to define appropriate standards for secure and effective use of this Organization's electronic mail systems, and internet usage in order to comply with the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, including updated HIPAA Laws, Rules and Regulations and State statutes and regulations concerning the privacy and security of Protected Health Information (PHI). There are myriad disparate other regulations for Personal Information (PI) and Sensitive Information

(SI) in regards to e-mail and internet usage. The same standards outlined in this policy for PHI may be adopted by this Organization, on a case by case basis for compliance with other regulations protecting PII or SI.

D. Policy

This Organization's electronic mail has become an integrated tool in this Organization's business processes. This policy defines the requirements for e-mail usage within this Organization. Electronic mail is designed to facilitate business communications and is not to be used in a way that may be disruptive, offensive to others or harmful to morale. Particular care must be given restricting the amount of PHI contained in any e-mails to the HIPAA Minimum Necessary and all e-mails containing PHI must be secured. This policy and all related procedures define the minimum requirements for Organization e-mail usage and are applicable to all Organization workforce members and includes PI and SI.

General Use – E-mail

This Organization's e-mail systems shall be used primarily for business use. Personal use of this Organization's e-mail systems shall be limited to a level that does not impede worker productivity. The content of all e-mails shall be used in a way that does not disrupt or offend others, harm morale or create security exposures. Members of this Organization workforce shall ensure that the business information contained in e-mail messages is accurate, appropriate and lawful. When sending e-mail attachment files, caution shall be taken by members of this Organization's workforce that the correct file is being attached. Recipient's authentication shall be performed (by the sender) prior to the transmission of all this Organization's e-mails to ensure that the content is only accessible by the intended recipient.

User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via this Organization's electronic mail system. Electronic mail is to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use e-mail appropriately, effectively, and efficiently. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

This Organization's e-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Right to Monitor E-mail and Communications

Management reserves the right to audit an employee's e-mail and communication system files (including e-mail files). Messages generated within and/or transmitted through this Organization's e-mail and/or communication systems are to be considered neither private

nor confidential. This Organization reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its e-mail or communication systems for any purpose. Upon separation of service, members of the Organization workforce shall not retain any rights to contents of this Organization's e-mail and/or communications systems. Additionally, all messages distributed via this Organization's e-mail and communication systems (including through non- Organization e-mail addresses) are subject to monitoring by Information Technology (I.T.), and disclosure to law enforcement or government officials or to other third parties through subpoena or other processes.

Electronic mail information is occasionally visible to I.T. staff engaged in routine testing, maintenance, and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of e-mail.

Management must advise and receive approval from the Human Resources Department, in conjunction with the HIPAA Security Officer, as appropriate, of their intent to review an employee's messages prior to accessing employee files.

Prohibited Uses

Certain activities are prohibited with regard to use of this Organization's e-mail and communication systems. The list below provides a framework for activities that fall into the category of unacceptable use. This list is not exhaustive and this Organization has the right to decide any activity is inappropriate at its discretion:

1. Organization email account should be used primarily for ORGANIZATION business-related purposes; personal communication is permitted on a limited basis, but non-ORGANIZATION related commercial uses are prohibited.
2. Using this Organization's e-mail and communication systems for effecting security breaches or disruptions of network communication.

3. Engaging in any activity that is illegal under local, state, federal or international law while utilizing any Organization I.T. or data.

4. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;

5. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.

6. Use of e-mail system for unauthorized solicitation of funds, political messages, gambling, commercial, or illegal activities.

7. Disclosure of an individual's personal information or a patient's Protected Health Information (PHI) without appropriate authorization.

8. Transmission of information to individuals inside or outside this Organization without a legitimate business need for the information.

9. Use of e-mail addresses for marketing purposes without explicit authorization from the target recipient.

10. Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of this Organization without the express authorization of counsel.

11. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.

12. Obtaining access to the files or communications of others with no substantial Organization business purpose and beyond the individual's 'need to know'.

13. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

14. Sending external transmission of confidential information via Organization e-mail and communication systems, including e-mail attachments without proper authorization, authentication and encryption.

15. Excessive personal use and/or unethical use of Organization's e-mail and communication systems.

16. Using Organization's electronic mail and other information systems, such as communication, in a way that may be disruptive, offensive to others or harmful to morale.

17. Opening, responding to, or forwarding e-mail messages from any unknown source.

18. Displaying or transmitting sexually explicit images, messages, games, cartoons or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, marital status, veteran status, age, disability or religious or political beliefs. E-mail is subject to this Organization policy and procedures governing sexual harassment and discrimination. Sending or forwarding offensive material violates this policy as well as the business use policy.

19. Using this Organization's e-mail and communication systems to solicit others for commercial ventures, religious or political causes, outside Organizations not approved of by this Organization, or in any other non-job-related situations. Sending chain letters or joke emails from an Organization email account is prohibited.

20. Circumventing user authentication or physical security controls to access this Organization's e-mail and communication systems.

21. Copying, transmitting or providing information about Organization e-mail and communication systems to any individual without proper authorization.

22. All Organization data contained within an email message or an attachment must be secured according to Organization policies and procedures.

23. Email should be retained only if it qualifies as an Organization business record. Email is a Organization business record if there is a legitimate and ongoing business reason to preserve the information contained in the email.

24. Email that is identified as an Organization business record shall be retained according to Organization Record Retention Schedule.

25. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Organization business, to create or memorialize any binding transactions, or to store or retain email on behalf of Organization. Such communications and transactions should be conducted through proper channels using Organization approved documentation.

This list is not considered all-inclusive or collectively exhaustive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or this Organization's HIPAA Privacy or Security Officer.

Confidentiality and Encryption of Electronic Mail

Users of this Organization's electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore, users are to utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents. When e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information.

Encryption of e-mails during data in transit and at rest is highly desirable for any sensitive or Protected Health Information (PHI), including patient identifiers and data. However, HIPAA does not require e-mail encryption per se. Rather the inducement for encryption is to place any e-mails encrypted according to HIPAA Security / NIST (National Institute of Standards and Technology) guidance will be considered to be in the 'Breach Safe Harbor' which eliminates the need for federal breach reporting and individual notification should a wrongful or inappropriate disclosure occur.

This Organization has considered the options for safeguarding our e-mails and has determined that the Organizational e-mails are to be encrypted.

These safeguards are as follows:

- Information considered confidential or sensitive should be, but is not required by HIPAA to be, protected during storage of the data utilizing encryption or password protection that ensures the information is not accessed by anyone other than the intended recipient.
- Encryption of e-mail in transit or as data at rest is not required, however it is strongly encouraged if the e-mail contains protected health information or otherwise sensitive information.
- Any PHI transmitted must be the Minimum Necessary amount, as defined by HIPAA Policy.
- Confidential or sensitive information is to be distributed only to those with a legitimate need to know, including multiple recipients.
- Never place patient identifiers or data within the subject line of e-mails.

The following statement is to be included on all *unencrypted* e-mail messages:

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Please be aware that unencrypted e-mail communications can be intercepted in transmission, misdirected or re-directed and read by unintended recipients and may constitute a breach of privacy under HIPAA. Your use of e-mail to communicate unencrypted sensitive or Protected Health Information (PHI) indicates that you acknowledge and accept the possible risks associated with such communication. Please consider communicating any sensitive information by a more secure means, including encrypted e-mail. If you do not wish to have your information sent by unencrypted e-mail, please contact the sender immediately.

The following statement is to be included on all e-mail *encrypted* e-mail messages:

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Retention of Electronic Mail

Generally, e-mail messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an e-mail message, it may be considered a more formal record and should be retained pursuant to this Organization's record retention schedules.

E-mail will not be routinely made a part of any client's medical records by this Organization. This would be E-mail will be included in medical records only if there is a note otherwise documented in the medical record indicating that this copy is necessary and there is a direct relationship to care rendered during the encounter for which the medical record is serving as the business record documenting that care. The clinician recording the mote about the e-mail is responsible for making sure a copy of the e-mail is placed into the medical record.

Electronic mail that users wish to or are required to retain must be moved to a permanent folder on their workstation.

Electronic mail tape back-ups are performed on a regular basis for the purpose of business recovery. Electronic mail tape back-ups are stored for (retention period) 7 years.

This Organization's Electronic Mail of Protected Health Information (PHI)

E-mailing confidential patient information necessary for the performance of your job is specifically authorized within this Organization's network if minimally necessary information is sent. Any e-mail communication of confidential patient information (protected health information) to non-Organization personnel or Organization personnel

outside the Organization network is specifically disallowed, except under the following conditions:

1. The request for this type of release has been forwarded to Clinical Resource Systems/Health Information Management for review and processing.

2. The patient/Designated Representative has signed a valid authorization specifically allowing such communication, and has been informed of all potential security risks and that this mode of transmission may not be secure. Organization staff will document such authorizations in the clinical record.

3. Verbal authorizations will be documented and witnessed on an authorization form by CRS/HIM, but are not considered an optimal method to communicate an authorization. If it is impractical to forward to CRS/HIM the request and rather than a verbal authorization, the e-mail authorization procedure listed below should be used.

4. The communication to an authorized recipient is accomplished in a way that it would be impossible to determine the identity of the patient if it were illegitimately intercepted.

5. The patient/designated representative must be informed that the authorization to release may be revoked at any time in writing, except to the extent it has been acted upon. The authorization will be effective only long enough to answer the purpose for which it is given, and no further confidential information will be released without the execution of an additional authorization.

All misdirected e-mail containing PHI must be documented and reported in accordance with the 'Information Security-Breach Notification Policy'.

E-mail Authorization Procedure

This procedure is recommended as opposed to verbal authorizations to communicate PHI and patient information via e-mail only if CRS/HIM reviews are not practical for a given circumstance.

This Organization may obtain informed consent from a patient or designated representative via e-mail by conducting the following consent exchange upon presentation of a patient query via electronic messaging (this example is for an e-mail exchange):

> I will be happy to respond to your query but to do so via e-mail you must provide your consent, recognizing that e-mail is not a secure form of communication. There is some risk that any protected health information that may be contained in such e-mail may be disclosed to, or intercepted by, unauthorized third parties. I will use the minimum necessary amount of protected health information to respond to your query.
>
> If you wish to conduct this discussion via e-mail, please indicate your acceptance of this risk with your e-mail reply. Alternatively, please call my office to arrange a phone conversation or office visit.

Note: that extra care should be taken by the sender to assure that the sender is confident of the correspondent's identity, that any PHI be kept to a minimum and that, as with phone or fax based exchanges, this consultation be documented in the patient's record if appropriate. Further, even when requested by a patient, the provider should decline to use e-mail and refer to phone or office visit if she or he has any concerns about any aspect of the exchange.

Texting of PHI

SMS and MMS type texting is totally prohibited for use with messages containing PHI. These methods can never be secured and have a host of other concerns (see CMS communications listed in 'References' section and a summary below). Encrypted e-mail may be allowable for PHI, but not for order.

CMS requires the following be functionalities which may be provided by secure texting services, but must be validated and risks analyzed according. However never can Orders be texted by any platform, CPOE is preferred and texting cannot replace verbal orders either.

Joint Commission likewise has come out with texting bans for physician orders.

CMS Memorandum Summary – 12/28/18

- Texting patient information among members of the health care team is permissible if accomplished through a secure platform.
- Texting of patient orders is prohibited regardless of the platform utilized.
- Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider.

§489.24(b) Standard: Form and retention of record. The hospital must maintain a medical record for each inpatient and outpatient. Medical records must be accurately written, promptly completed, properly filed and retained, and accessible. The hospital must use a system of author identification and record maintenance that ensures the integrity of the authentication and protects the security of all record entries. (1) Medical records must be retained in their original or legally reproduced form for a period of at least 5 years. And (3) The hospital must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with Federal or State laws, court orders, or subpoenas.

Allowed Internet Activities and Services

Organization Business information that is accessed via the internet is to be used for business purposes only. Capabilities for the following standard internet services will be provided to users as needed:

- E-mail -- Send/receive E-mail messages to/from the internet (with or without document attachments).

- Navigation – www type internet services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the internet; limited access from the internet to dedicated company public web servers only.

- File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.

Management reserves the right to add or delete services as business needs change or conditions warrant.

All other services will be considered unauthorized access to/from the internet and will not be allowed.

Request & Approval Procedures

Access to Organization Business information will be provided to users to support business activities and only as needed to perform their jobs.

Request for Access

As part of the access request process, the employee has been trained on the e-mail and internet use policies and procedures. Users not complying with these policies could be subject to disciplinary action up to and including termination.

Approval

Access is requested by the user or user's manager by submitting an approved IT Access Request Form.

Removal of privileges

Access will be discontinued immediately upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

Allowed Usage

Access and usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the internet.

Acceptable use of the internet for performing job functions may include, but not be limited to the following. Any questions of whether a type of access or use of the internet can be addressed by IT or the Security Officer:

- Communication between employees and non-employees for business purposes;

- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information.
- Research

Personal Use of the Internet

Using company IT and network resources to access the internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Prohibited Internet Use

Any consequential loss of personal information or property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing Organization Business Information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of company Web sites to other internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or Organization. Assume that all materials on the internet are copyright and/or patented unless specific notices state otherwise.

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.

Software License

The company strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to management before any copying is done.

Similarly, reproduction of copyrighted materials available over the internet must be done only with the written permission of the author or owner of the document, if appropriate. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary or the information was distribute for public consumption. This notion of "fair use" is in keeping with international copyright laws.

Using company computer resources to access the internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

Monitoring

Users should consider their internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, workforce member internet usage personal file directories, web access, and other information stored on company networks and IT equipment, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

Policy Compliance

- Organization management may utilize both internal and external resources to verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to management.
- Any exception to the policy must be approved by management in advance.
- An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Responsibilities

<u>Organization Management</u>

This Organization's management shall ensure their staff adheres to the requirements outlined in this policy and all subordinate procedures related to e-mail, communication

systems and internet usage. Management must immediately report any known or suspected breach of a privacy or security policy to the HIPAA Privacy or Security Officer.

Organization Workforce

All workforce members shall comply with this policy and all referenced policies to ensure privacy of sensitive information. Members of this Organization's workforce shall report any known or suspected breach of this policy and/or its subordinate procedures to management or the HIPAA Privacy or Security Officer.

Organization Business Associates / Sub-contractors

All Business Associates / sub-contractors of this Organization shall comply with this policy to ensure the privacy and security of Protected Health Information (PHI). Any known breach, shall be immediately reported to the HIPAA Security or Privacy Officer.

Organization Information Technology (IT)

IT shall maintain and update all policies related to e-mail and communication system usage to ensure that they are comprehensive and consistent with local, state, federal and international law. I.T. shall ensure that all responsibilities for carrying out the requirements outlined within this policy are delegated to qualified staff. I.T. reserves the right to intercept, monitor, access, and/or disclose any information that is maintained on, stored in or transmitted through its e-mail or communication systems for any purpose. The Privacy or Security Officer shall be made aware of any breach of security policy and advise Human Resources.

Accountability

All Organization workforce members with access to this Organization's information systems who are found to be in violation of any part of this policy are subject to disciplinary action, up to and including termination of employment or contract and legal action. I.T. will immediately suspend e-mail system access privileges to any authorized user when unacceptable use severely impacts system performance or security. Retaliatory action shall not be taken against individuals who identify and/or report violations of security policy.

E. Related Policies

- 21s – Breach Determination and Reporting
- 6s – Appropriate Access to PHI by Workforce
- 2s – Documentation for Privacy Compliance
- 26s – Sanctions, Enforcement and Discipline

- 117s – Integrity Controls Including Encryption

F. References

- HIPAA Security Rule 45 CFR §164.308
- CompliancePro Solutions™ HIPAA Security Risk Analysis™ (SRA)
- SRA Line Item Number: D34
- NIST 800-53 Recommended Security Controls for federal Systems
- 45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information
- Memo on Texting from CMS 12/28/17 Ref: S&C 18-10-ALL: Texting of Patient Information among Healthcare Providers.

Fax Transmissions

A. Coverage

Endodontic Associates (hereafter referred to as the 'Organization') workforce members (i.e. employees, contractors and volunteers) who utilize Fax technology for the disclosure of Protected Health Information (PHI).

B. Create / Revision Date

February 11, 2026

C. Purpose

Ensure that fax technology is utilized as minimally as possible, and with proper procedures, to maintain PHI Privacy during fax disclosures.

D. Policy

As the facsimile transmission of information has become common in the health care industry, the Organization has adopted this policy for the control of health information transmittal, which is deemed 'unsecure' by HIPAA Privacy and Security Rules, which

means that misdirected faxes are subject to Privacy Breach Notification, which is highly undesirable.

1. Facsimile transmission (fax) of medical records should be limited to use by health care providers for treatment purposes only or upon written request of the patient to receive their PHI via this method. Fax is an inherently 'unsecured' method of communicating patient information (defined as Protected Health Information or 'PHI') and therefore per HIPAA Privacy Rules should be restricted to the minimum possible.

2. Options to fax, such as *secure* e-mails (with encryption according to HIPAA Security Rules) should be utilized, if available, in lieu of faxes.

3. The facsimile transmission of patient information should be sent or received to a device that is manned by authorized health care personnel or designated by the patient in the written request. The device should also be located in a secured area where unauthorized access is avoided.

4. Procedures shall be followed to ensure correct transmission and receipt of faxes by intended recipient are confirmed.

5. A fax cover sheet should always be utilized when faxing patient information outside the Organization that has the following items completed: date, fax telephone number, name of recipient, name of sender, and any appropriate comments regarding the information.

    a. Develop a Confidential Fax Coversheet to provide extra protection for PHI and demonstrate your due diligence in this area. The headline of the coversheet should state in large bold type: "Confidential Health Information Enclosed." Beneath this headline, include a statement such as: Health Care Information is personal and sensitive information related to a person's health care. It is being faxed to you after appropriate authorization from the patient or under circumstances that doesn't require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure and confidential manner. Re-disclosure without additional patient consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law.

    b. Include at the bottom of the fax coversheet a warning such as: IMPORTANT WARNING: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and

confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is STRICTLY PROHIBITED. If you have received this message by error, please notify us immediately and destroy the related message.

c. In addition to the warnings described in (3) and (4) above, make sure the fax coversheet contains standard information including:

    1. Date and time of the fax
    2. Sender's name, address, telephone number and fax number
    3. The authorized recipient's name, telephone number and fax number
    4. Number of pages transmitted
    5. Information regarding verification of receipt of the fax.

6. Whenever possible, auto-faxing should be utilized for reduction of human errors in dialing the fax telephone numbers. However, auto fax numbers must be tested and audited regularly to ensure their validity.

7. Records of a privileged nature, as protected by Federal Law and State Statutes, specifically psychiatric, drug/alcohol abuse, AIDS, and AIDS related conditions, and HIV tests and information, should receive special consideration. Records of this nature should not be faxed except in an extreme emergency.

8. On a regular basis all fax machines with auto-faxing capabilities should be audited for correct numbers and processing of faxes with test results being retained as part of ongoing HIPAA Privacy compliance records.

Fax and Mailing Checklist Guidelines from HHS

These guidelines were published by HHS to aid in faxing and mailing to help prevent wrongful disclosure by sending unencrypted PHI to the wrong, non-patient parties. Generally, the Privacy Rule permits a covered entity to make disclosures of protected health information (PHI) for a permitted purpose, through a variety of means, such as by mail or facsimile machine, as long as the covered entity, when doing so, uses reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of the PHI. These safeguards may vary depending on the mode of communication used. For example, when faxing PHI to a telephone number that is not used regularly, a reasonable safeguard may involve a covered entity

Q: May a physician's office or health plan use mail or fax to send patient medical information?

A: Yes. Where the Privacy Rule allows covered health care providers, health plans, or health care clearinghouses to share protected health information with another organization or with the individual, they may use a variety of means to deliver the information, as long as they use reasonable safeguards when doing so. When the communications are in writing, the patient information may be sent by mail, fax, or other means of reliable delivery.

The Privacy Rule requires that covered entities apply reasonable safeguards when making these communications to protect the patient information from inappropriate use or disclosure to unauthorized persons. These safeguards will vary depending on the mode of communication used. For example, when mailing patient information, reasonable safeguards would include checking to see that the name and address of the recipient are correct and current and that only the minimum amount of patient information is showing on the outside of the envelope to ensure proper delivery to the intended recipient. When faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard would include first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information to someone who is not the intended recipient. The following checklists provide guidance on reasonable safeguards that a covered health care provider, health plan, or health care clearinghouse may put in place to protect patient information from being impermissibly disclosed during (1) mailing and (2) faxing.

MAILING CHECKLIST
Carefully check name and address of intended recipient. Many names are similar; make sure you have the correct name for the intended recipient on the envelope. Make sure the address on the envelope matches the correct address of the intended recipient.
Carefully check the contents of the envelope before sealing. Make sure the contents may be permissibly disclosed to the intended recipient or properly relate to the individual. Check all pages to make sure records or material related to other individuals are not mistakenly included in the envelope.
Check the information showing on the outside of the envelope or through the address window. Make sure identifying information that is not necessary to ensure proper delivery is not disclosed.
When doing mass mailings, do test runs to ensure the system is properly performing and check at least a sample of the mailings for the accuracy of name and address of the intended recipients and the correct contents, as indicated above before sending.
Have policies and procedures in place to safeguard protected health information that is mailed, including processes to act promptly on (1) name and address

changes to ensure corrections are made in all the relevant records; and (2) reports of misdirected mail to identify the cause and take steps to prevent future incidents.
Train staff on the mailing procedures that your organization has put in place to safeguard protected health information during mailing. Update the training periodically and be sure to train new staff.
FAXING CHECKLIST
Carefully check the fax number to make sure you have the correct number for the intended recipient. When manually entering the number, check to see that it has been entered correctly before sending.
Confirm fax number with the intended recipient when faxing to this party for the first time or if the fax number is not regularly used.
Program regularly used numbers into fax machines. Check to make sure you are selecting the preprogrammed number for the correct party before sending.
Update fax numbers promptly upon receipt of notification of correction or change. Have procedures for deleting outdated or unused numbers which are preprogrammed into the fax machine.
Locate fax machines in areas where access can be monitored and controlled and avoid leaving patient information on fax machines after sending.
Have policies and procedures in place to safeguard protected health information that is faxed, including processes to act promptly on (1) changes in fax numbers to ensure corrections are made in all the relevant records; and (2) reports of a misdirected fax to identify the cause and take steps to prevent future incidents, including revising the organization's policies and procedures.
Train staff on the policies and procedures for the proper use of fax machines that your organization has put in place to safeguard protected health information during faxing. Update the training periodically and be sure to train new staff.

E. Related Forms

- Fax Cover Sheet

F. Related Polices

- 11s – Disclosure of PHI
  List additional related polices

G. References

PRA Line Item: C.35, L.3, L.4

NOTICE OF PRIVACY PRACTICES – Spanish Version

AVISO DE PRÁCTICAS DE PRIVACIDAD – Este aviso describe cómo la información médica sobre usted puede ser utilizada y divulgada y cómo puede obtener acceso a esta información. POR FAVOR, REVÍSELO CUIDADOSAMENTE.

Este Aviso entra en vigor el 02/10/2026 y reemplaza todas las versiones anteriores.

I.

Nuestra organización está comprometida a proteger la información de salud sobre usted. Creamos un registro de la atención médica y los servicios que usted recibe en Endodontic Associates para su cuidado y tratamiento. Necesitamos este registro para brindarle atención de calidad y para cumplir con ciertos requisitos legales.

Este aviso se aplica a todos los registros de su atención relacionados con los servicios prestados en hospitales, centros de atención ambulatoria y otras instalaciones que conforman Endodontic Associates, así como a los médicos y otros profesionales de la salud que prestan servicios dentro de dichas entidades. Si su proveedor personal de atención médica (proveedor) no es empleado de Endodontic Associates, su proveedor puede tener políticas o Avisos diferentes con respecto a cómo se utiliza o divulga la información mantenida en su consultorio o clínica.

La ley nos exige:
• Asegurarnos de que su información de salud esté protegida;
• Entregarle este Aviso que describe nuestras obligaciones legales para proteger su privacidad;
• Cumplir con los términos del Aviso que esté actualmente en vigor; y
• Notificarle en caso de una violación de su información médica protegida no asegurada (PHI, por sus siglas en inglés), según lo requiera la ley.

Usted tiene derecho a recibir una copia de este Aviso y comentarlo con nuestra Oficina de Privacidad llamando al número o escribiendo a la dirección que aparecen al final de este Aviso.

II. CÓMO PODEMOS UTILIZAR Y DIVULGAR SU INFORMACIÓN MÉDICA PROTEGIDA

Las siguientes secciones describen las maneras en que podemos utilizar y divulgar su información médica protegida. Para cada categoría, describiremos los usos y daremos algunos ejemplos. Cierta información, como información genética, información relacionada con drogas y alcohol, información sobre VIH y salud mental, puede estar sujeta a restricciones especiales

conforme a las leyes estatales y federales. Cumplimos con todas las leyes estatales y federales aplicables relacionadas con la protección de esta información. No se enumerarán todos los usos o divulgaciones posibles; sin embargo, todos los usos y divulgaciones permitidos estarán dentro de una de las siguientes categorías.

A. Para Tratamiento

Podemos utilizar su información médica protegida para brindarle tratamiento o servicios. Podemos divulgar su información de salud a otros profesionales involucrados en su atención, agencias o instalaciones no afiliadas a Endodontic Associates para proporcionar o coordinar los diferentes servicios que usted necesite, como recetas, análisis de laboratorio y radiografías. También podemos divulgar esta información a personas involucradas en su cuidado. Podemos comunicarnos con usted para recordatorios de citas, obtener información de registro del paciente, informarle sobre alternativas de tratamiento u otros beneficios y servicios relacionados con la salud que puedan interesarle, o para dar seguimiento a su atención.

B. Para Pago

Podemos utilizar y divulgar su información médica protegida para actividades de facturación y pago de Endodontic Associates y otros involucrados en su atención, como una compañía de ambulancias. Por ejemplo, podemos usar y divulgar información para que Endodontic Associates u otros puedan obtener el pago de usted, una compañía de seguros u otro tercero. También podemos informar a su aseguradora sobre un tratamiento que necesite para obtener autorización previa o verificar si su seguro cubrirá el tratamiento.

C. Para Operaciones de Atención Médica

Podemos utilizar y divulgar su información de salud para nuestras operaciones de atención médica, que incluyen diversas actividades necesarias para administrar nuestro negocio, brindar servicios de atención médica de calidad y comunicarnos con usted cuando sea necesario. Podemos divulgar su información médica protegida a estudiantes de medicina o enfermería y otros aprendices con fines de revisión y aprendizaje.

D. Intercambio de Información de Salud (HIE)

Podemos participar en un Intercambio Electrónico de Información de Salud (“HIE”) para facilitar el intercambio de su información médica protegida con fines de tratamiento. Un HIE es una red en la que los proveedores intercambian información del paciente para facilitar la atención médica.

E. Asociados Comerciales y Proveedores de Servicios

Podemos divulgar su información médica protegida a terceros denominados “Asociados Comerciales”. Estos brindan diversos servicios a Endodontic Associates o en su nombre, como servicios de facturación, transcripción y servicios legales. Nos aseguramos de que todos los Asociados Comerciales y proveedores de servicios, independientemente de su ubicación, estén

obligados a proteger su PHI conforme a las leyes de los Estados Unidos e internacionales, incluida la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA).

F. Requerido por Ley

Divulgaremos su información médica protegida cuando lo exijan las leyes federales, estatales o locales. Esto incluye, entre otros, reportes a registros obligatorios de pacientes, notificación de eventos adversos a la Administración de Alimentos y Medicamentos (FDA), actividades de supervisión de la salud pública, prevención de enfermedades, retiros de productos del mercado, sospecha de abuso o violencia doméstica, y cumplimiento de órdenes judiciales o citaciones legales.

G. Investigación

Podemos utilizar y divulgar su información médica protegida con fines de investigación conforme a las leyes federales y estatales aplicables. Todos los proyectos de investigación están sujetos a un proceso especial de aprobación para garantizar la protección de su información. Cuando sea necesario, obtendremos su autorización por escrito antes de usar o divulgar su información para investigación.

H. Información sobre Trastornos por Uso de Sustancias (SUD)

Si recibimos o mantenemos información suya proveniente de un programa de tratamiento SUD cubierto por 42 CFR Parte 2, podremos usar y divulgar dicha información para tratamiento, pago u operaciones de atención médica según lo descrito en este Aviso, conforme al consentimiento proporcionado. En ningún caso utilizaremos o divulgaremos su información SUD en procedimientos civiles, penales, administrativos o legislativos en su contra sin su consentimiento o una orden judicial válida.

I. Directorios de Instalaciones (solo pacientes hospitalizados)

A menos que usted se oponga, podremos incluir su nombre, ubicación y condición general en nuestro directorio para que familiares, amigos o miembros del clero puedan visitarlo y conocer su estado general.

J. Personas Involucradas en su Atención

A menos que usted indique lo contrario, podremos divulgar su información de salud a personas involucradas en su atención o pago, como familiares o amigos.

K. Procedimientos y Acciones Legales

Podemos divulgar su información médica protegida en respuesta a órdenes judiciales, citaciones u otros procesos legales válidos.

L. Actividades de Recaudación de Fondos

Podemos comunicarnos con usted para recaudar fondos e informarle sobre actividades de Endodontic Associates. Puede solicitar no recibir estas comunicaciones enviando un correo a billing@sanmateoendo.com o llamando al (650) 340-0225.

M. Situaciones Especiales

Incluyen ayuda en casos de desastre, donación de órganos, compensación laboral, seguridad nacional, actividades militares y servicios de protección presidencial.

N. Inteligencia Artificial (IA)

Podemos utilizar tecnología de IA para apoyar decisiones operativas y recomendaciones sobre su tratamiento o atención. Los socios tecnológicos de IA están obligados a mantener su información confidencial.

O. (Si Aplica) Intercambio dentro de un OHCA

Mantenemos su registro electrónico de salud (EHR) junto con otras entidades participantes en un Arreglo Organizado de Atención Médica (OHCA). Las entidades participantes pueden usar y divulgar información para tratamiento, pago y operaciones de atención médica.

III. DERECHO DE ACCESO

Tiene derecho a acceder a su información médica protegida comunicándose con la ubicación donde recibió atención o llamando al número indicado al final de este Aviso.

También le pedimos que respete la privacidad de otros pacientes mientras se encuentre en nuestras instalaciones.

Sus Derechos

Usted tiene derecho a:

A. Inspeccionar y obtener copia electrónica o en papel de su información médica protegida.
B. Solicitar una enmienda si considera que la información es incorrecta o incompleta.
C. Solicitar un informe de ciertas divulgaciones realizadas en los últimos seis (6) años.
D. Solicitar restricciones sobre el uso o divulgación de su información.
E. Obtener una copia impresa de este Aviso en cualquier momento.
F. Designar a una persona para que actúe en su nombre (por ejemplo, con poder notarial médico).

IV. Usos que Requieren Autorización

A. Notas de Psicoterapia – Requieren autorización escrita, salvo excepciones legales.
B. Mercadeo – Requiere autorización escrita salvo excepciones específicas. El consentimiento para recibir mensajes no será compartido ni vendido con fines de marketing.
C. Venta de Información Médica – Requiere autorización escrita si hay remuneración.
D. Otros Usos – Cualquier otro uso no descrito requerirá su autorización escrita, la cual puede revocar en cualquier momento.

V. CAMBIOS A ESTE AVISO

Nos reservamos el derecho de modificar este Aviso y nuestras prácticas de privacidad. El Aviso revisado estará disponible a solicitud y en nuestro sitio web.

VI. PREGUNTAS/QUEJAS

Si considera que sus derechos de privacidad han sido violados, puede presentar una queja sin temor a represalias.

Marnie Burse
Endodontic Associates
(650) 340-0225
billing@sanmateoendo.com
235 N. San Mateo Dr., Ste. 400
San Mateo, CA 94401

O con el Secretario del Departamento de Salud y Servicios Humanos:

U.S. Dept. of Health and Human Services
Office for Civil Rights
2000 Independence Avenue, S.W.
Washington, D.C. 20201
1-877-696-6775

Política de Uso de Correo Electrónico, Mensajería de Texto e Internet

---

A. Alcance

Endodontic Associates (en adelante, la “Organización”) —incluyendo miembros de la fuerza laboral, trabajadores contratados, personal de agencias temporales, socios comerciales y proveedores— que accedan, utilicen o divulguen información confidencial de pacientes y/o de la empresa.

B. Revisado/Actualizado

11 de febrero de 2026

C. Propósito

La Regla de Seguridad de HIPAA especifica que las entidades cubiertas deben “implementar medidas técnicas de seguridad para proteger contra el acceso no autorizado a la e-PHI que se transmite a través de una red de comunicaciones electrónicas” y “implementar procedimientos para verificar que una persona o entidad que solicita acceso a ePHI es quien dice ser”.

El propósito de esta política es definir estándares apropiados para el uso seguro y eficaz de los sistemas de correo electrónico y del uso de Internet de esta Organización, con el fin de cumplir con los estándares de privacidad y seguridad establecidos por la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) de 1996, incluidas sus leyes, normas y reglamentos actualizados, así como los estatutos y regulaciones estatales relacionados con la privacidad y seguridad de la Información de Salud Protegida (PHI).

Existen numerosas regulaciones adicionales relacionadas con Información Personal (PI) e Información Sensible (SI) en cuanto al uso de correo electrónico e Internet. Los mismos estándares descritos en esta política para la PHI podrán adoptarse caso por caso para cumplir con otras regulaciones que protejan la Información de Identificación Personal (PII) o Información Sensible (SI).

D. Política

El correo electrónico se ha convertido en una herramienta integrada en los procesos comerciales de esta Organización. Esta política define los requisitos para el uso del correo electrónico dentro de la Organización. El correo electrónico está diseñado para facilitar las comunicaciones comerciales y no debe utilizarse de manera disruptiva, ofensiva o perjudicial para la moral.

Se debe tener especial cuidado en limitar la cantidad de PHI contenida en cualquier correo electrónico al “Mínimo Necesario” conforme a HIPAA, y todos los correos que contengan PHI deben estar protegidos.

Esta política y todos los procedimientos relacionados definen los requisitos mínimos para el uso del correo electrónico de la Organización y son aplicables a todos los miembros de la fuerza laboral, incluyendo PI y SI.

Uso General – Correo Electrónico

Los sistemas de correo electrónico de la Organización deben utilizarse principalmente para fines comerciales. El uso personal deberá limitarse a un nivel que no afecte la productividad laboral.

El contenido de todos los correos electrónicos deberá utilizarse de manera que no ofenda a otros, no perjudique la moral ni genere riesgos de seguridad. Los miembros de la fuerza laboral deberán asegurarse de que la información comercial contenida en los mensajes sea precisa, apropiada y legal.

Al enviar archivos adjuntos, se debe verificar que el archivo correcto esté siendo enviado. El remitente deberá autenticar al destinatario antes de la transmisión para garantizar que el contenido sea accesible únicamente para el receptor previsto.

Responsabilidades del Usuario

Se considera usuario a cualquier persona autorizada para leer, ingresar o actualizar información creada o transmitida mediante el sistema de correo electrónico de la Organización.

El correo electrónico debe utilizarse como herramienta comercial para facilitar la comunicación necesaria para el desempeño del trabajo. El uso personal incidental es permisible siempre que:
(a) no consuma más que una cantidad trivial de recursos;
(b) no interfiera con la productividad; y
(c) no sustituya actividades comerciales.

Los usuarios deben ejercer discreción y aplicar protecciones de confidencialidad iguales o superiores a las utilizadas en documentos escritos.

Las cuentas y contraseñas de correo electrónico no deben compartirse ni divulgarse a personas no autorizadas.

Derecho a Monitorear

La administración se reserva el derecho de auditar los archivos de correo electrónico y comunicaciones. Los mensajes generados o transmitidos mediante los sistemas de la Organización no se consideran privados ni confidenciales.

La Organización podrá interceptar, monitorear, acceder o divulgar información almacenada o transmitida por sus sistemas por cualquier motivo.

Al finalizar la relación laboral o contractual, el personal no conservará derechos sobre el contenido del correo electrónico de la Organización.

Usos Prohibidos

Las siguientes actividades están prohibidas (lista no exhaustiva):

1. Uso del correo para fines comerciales no relacionados con la Organización.
2. Intentos de vulnerar la seguridad o interrumpir redes.
3. Actividades ilegales bajo cualquier ley aplicable.
4. Copiar o transmitir materiales protegidos por derechos de autor sin autorización.
5. Comunicaciones amenazantes, difamatorias, obscenas u ofensivas.
6. Solicitudes no autorizadas de fondos, mensajes políticos o actividades comerciales externas.
7. Divulgación de PHI sin autorización apropiada.
8. Transmisión de información sin necesidad comercial legítima.
9. Uso de direcciones de correo para fines de marketing sin autorización explícita.
10. Reenvío de correos de asesoría legal sin autorización expresa.
11. Suplantación o alteración de identidad en comunicaciones electrónicas.
12. Acceso no autorizado a archivos o comunicaciones.
13. Intentos de acceso no autorizado a datos o sistemas.
14. Envío externo de información confidencial sin autorización, autenticación y cifrado adecuados.
15. Uso personal excesivo o poco ético.
16. Uso disruptivo u ofensivo.
17. Apertura o reenvío de correos de fuentes desconocidas.
18. Envío de contenido sexual explícito o discriminatorio.
19. Envío de cadenas o correos de bromas.
20. Elusión de controles de autenticación o seguridad física.
21. Divulgación no autorizada de información sobre sistemas de correo.
22. Falta de protección de datos de la Organización en correos o adjuntos.
23. Retener correos solo si califican como registros comerciales.
24. Retener registros conforme al calendario de retención.
25. Uso de servicios de correo de terceros (Google, Yahoo, Hotmail, etc.) para negocios de la Organización.

Confidencialidad y Cifrado

Los usuarios deben aplicar medidas de confidencialidad equivalentes o superiores a las de documentos escritos.

El cifrado del correo electrónico es altamente recomendable para PHI. Aunque HIPAA no exige específicamente el cifrado, los correos cifrados conforme a las guías de HIPAA/NIST pueden calificar bajo el “Puerto Seguro de Violación (Breach Safe Harbor)”.

La Organización ha determinado que sus correos electrónicos deben estar cifrados.

Salvaguardas:

- Utilizar cifrado o protección con contraseña para información sensible.
- Limitar la PHI al mínimo necesario.
- Distribuir información confidencial solo a quienes tengan necesidad legítima.
- No incluir identificadores de pacientes en la línea de asunto.

Aviso de Confidencialidad (para correos no cifrados y cifrados):
Este mensaje de correo electrónico, incluidos los archivos adjuntos, es para uso exclusivo del destinatario previsto y puede contener información confidencial y privilegiada. Cualquier revisión, uso o divulgación no autorizada está prohibida. Si usted no es el destinatario previsto, comuníquese con el remitente y destruya todas las copias del mensaje original.

Retención del Correo Electrónico

En general, los correos electrónicos constituyen comunicaciones temporales y pueden descartarse rutinariamente, salvo que su contenido requiera retención conforme al calendario de registros.

Las copias de seguridad se conservan por un período de 7 años.

PHI y Correo Electrónico

El envío de información confidencial del paciente es autorizado únicamente dentro de la red de la Organización y bajo el estándar de “mínimo necesario”.

El envío a personal externo está prohibido salvo que:

- Exista autorización válida firmada.
- Se haya informado al paciente sobre riesgos de seguridad.
- La autorización pueda revocarse por escrito.

Todo correo mal dirigido que contenga PHI debe documentarse y reportarse conforme a la Política de Notificación de Brechas.

Mensajería de Texto (Texting)

El uso de SMS o MMS para PHI está totalmente prohibido.

CMS establece que:

- El envío de información del paciente entre miembros del equipo es permisible solo mediante plataforma segura.
- Está prohibido enviar órdenes médicas por mensaje de texto.
- CPOE es el método preferido para órdenes.

Actividades Permitidas en Internet

El acceso a Internet es exclusivamente para fines comerciales.
Servicios permitidos incluyen:

- Correo electrónico
- Navegación web (HTTP)
- Transferencia de archivos (FTP)

Otros servicios se considerarán no autorizados.

Cumplimiento y Responsabilidades

Administración: Garantizar cumplimiento y reportar brechas.
Fuerza Laboral: Cumplir y reportar violaciones.
Asociados Comerciales: Cumplir y reportar brechas.
Tecnología de la Información (IT): Mantener políticas actualizadas y monitorear sistemas.

Responsabilidad

Las violaciones pueden resultar en acciones disciplinarias, incluyendo despido y acciones legales. IT podrá suspender inmediatamente el acceso ante uso inaceptable. No se tomarán represalias contra quienes reporten violaciones.

E. Políticas Relacionadas

- 21s – Determinación y Reporte de Brechas
- 6s – Acceso Apropiado a PHI
- 2s – Documentación para Cumplimiento de Privacidad
- 26s – Sanciones y Disciplina
- 117s – Controles de Integridad, incluido Cifrado

F. Referencias

- HIPAA Security Rule 45 CFR §164.308
- NIST 800-53
- 45 CFR Partes 160 y 164
- Memorando CMS 12/28/17 S&C 18-10-ALL

Si deseas, puedo formatearlo como documento oficial listo para impresión (con encabezados corporativos y formato legal profesional).

Transmisiones por Fax

A. Cobertura

Los miembros de la fuerza laboral de Endodontic Associates (en adelante, la "Organización") (es decir, empleados, contratistas y voluntarios) que utilicen tecnología de fax para la divulgación de Información de Salud Protegida (PHI, por sus siglas en inglés).

B. Fecha de creación / revisión

11 de febrero de 2026

C. Propósito

Garantizar que la tecnología de fax se utilice lo menos posible y siguiendo los procedimientos adecuados para mantener la privacidad de la PHI durante su divulgación por fax.

D. Política

Dado que la transmisión de información por fax se ha vuelto común en la industria de la salud, la Organización ha adoptado esta política para el control de la transmisión de información de salud, la cual se considera "no segura" según las Reglas de Privacidad y Seguridad de HIPAA. Esto significa que los faxes enviados por error están sujetos a Notificación de Violación de Privacidad, lo cual es altamente indeseable.

1. La transmisión por fax de expedientes médicos debe limitarse al uso entre proveedores de atención médica únicamente con fines de tratamiento, o previa solicitud por escrito del paciente para recibir su PHI por este medio. El fax es un método inherentemente "no seguro" para comunicar información del paciente (definida como Información de Salud Protegida o "PHI") y, por lo tanto, conforme a las Reglas de Privacidad de HIPAA, debe restringirse al mínimo posible.
2. Siempre que estén disponibles, deben utilizarse alternativas al fax, como correos electrónicos seguros (con cifrado conforme a las Reglas de Seguridad de HIPAA), en lugar del fax.
3. La transmisión por fax de información del paciente debe enviarse o recibirse en un dispositivo atendido por personal autorizado de atención médica o designado por el paciente en la solicitud por escrito. El dispositivo también debe estar ubicado en un área segura donde se evite el acceso no autorizado.
4. Deben seguirse procedimientos para garantizar que la transmisión y recepción correctas del fax por el destinatario previsto sean confirmadas.
5. Siempre debe utilizarse una hoja de portada al enviar por fax información del paciente fuera de la Organización, la cual debe incluir: fecha, número de fax, nombre del destinatario, nombre del remitente y cualquier comentario apropiado sobre la información.

   a. Desarrollar una Hoja de Portada de Fax Confidencial para brindar protección adicional a la PHI y demostrar diligencia debida en esta área. El encabezado debe indicar en letras grandes y en negrita: "Información de Salud Confidencial Adjunta". Debajo del encabezado, incluir una declaración como la siguiente:
   La información de atención médica es información personal y sensible relacionada con la atención médica de una persona. Se le envía por fax después de la autorización correspondiente del paciente o en circunstancias que no requieren autorización del paciente. Usted, como destinatario, está obligado a mantenerla de manera segura y confidencial. La redistribución sin consentimiento adicional del paciente o sin estar permitida por la ley está prohibida. La redistribución no autorizada o el incumplimiento de mantener la confidencialidad puede someterle a sanciones descritas en la ley federal y estatal.

   b. Incluir al final de la hoja de portada una advertencia como la siguiente:
   ADVERTENCIA IMPORTANTE: Este mensaje está destinado únicamente para el uso de la persona o entidad a la que va dirigido y puede contener información privilegiada y confidencial, cuya divulgación está regulada por la ley aplicable. Si el lector de este mensaje no es el destinatario previsto, ni el empleado o agente responsable de entregarlo al destinatario previsto, se le notifica por la presente que cualquier divulgación, distribución o copia de esta información está ESTRICTAMENTE PROHIBIDA. Si ha

recibido este mensaje por error, notifíquenos de inmediato y destruya el mensaje correspondiente.

c. Además de las advertencias descritas anteriormente, asegurarse de que la hoja de portada incluya la siguiente información estándar:

1. Fecha y hora del fax
2. Nombre, dirección, número de teléfono y número de fax del remitente
3. Nombre, número de teléfono y número de fax del destinatario autorizado
4. Número de páginas transmitidas
5. Información sobre la verificación de recepción del fax

6. Siempre que sea posible, debe utilizarse la función de marcación automática para reducir errores humanos al marcar números de fax. Sin embargo, los números programados deben probarse y auditarse regularmente para garantizar su validez.
7. Los registros de naturaleza privilegiada protegidos por la ley federal y los estatutos estatales, específicamente los psiquiátricos, de abuso de drogas/alcohol, SIDA y condiciones relacionadas con el SIDA, así como pruebas e información sobre VIH, deben recibir consideración especial. Este tipo de registros no debe enviarse por fax excepto en una emergencia extrema.
8. De manera regular, todas las máquinas de fax con capacidad de marcación automática deben auditarse para verificar números correctos y procesamiento adecuado de faxes, conservando los resultados de prueba como parte de los registros continuos de cumplimiento de privacidad HIPAA.

Guías de Lista de Verificación para Fax y Correo del HHS

Estas guías fueron publicadas por el HHS para ayudar en el envío por fax y correo con el fin de prevenir la divulgación indebida al enviar PHI no cifrada a personas que no sean el paciente previsto. En general, la Regla de Privacidad permite que una entidad cubierta divulgue PHI para un propósito permitido, a través de diversos medios como correo o fax, siempre que utilice salvaguardas administrativas, técnicas y físicas razonables y apropiadas para proteger la privacidad de la PHI. Estas salvaguardas pueden variar según el medio de comunicación utilizado.

Pregunta: ¿Puede el consultorio de un médico o un plan de salud usar correo o fax para enviar información médica del paciente?
Respuesta: Sí. Cuando la Regla de Privacidad permite que proveedores de atención médica cubiertos, planes de salud o cámaras de compensación compartan PHI con otra organización o con el individuo, pueden utilizar diversos medios para entregar la información, siempre que empleen salvaguardas razonables.

La Regla de Privacidad exige que las entidades cubiertas apliquen salvaguardas razonables para proteger la información del paciente contra uso o divulgación inapropiada. Estas salvaguardas variarán según el medio utilizado.

Por ejemplo:

- Al enviar información por correo, las salvaguardas razonables incluyen verificar que el nombre y la dirección del destinatario sean correctos y actuales, y que solo la cantidad mínima necesaria de información del paciente sea visible en el exterior del sobre.
- Al enviar PHI por fax a un número que no se utiliza regularmente, una salvaguarda razonable incluye confirmar primero el número con el destinatario previsto.
- También pueden programarse números utilizados con frecuencia en la máquina de fax para evitar errores.

LISTA DE VERIFICACIÓN PARA ENVÍO POR CORREO

- Verificar cuidadosamente el nombre y la dirección del destinatario previsto.
- Confirmar el contenido del sobre antes de sellarlo.
- Revisar que no se incluya información de otros individuos por error.
- Asegurarse de que la información visible en el exterior del sobre no revele datos innecesarios.
- Realizar pruebas en envíos masivos y revisar muestras antes de enviar.
- Implementar políticas y procedimientos para actuar rápidamente ante cambios de nombre/dirección y reportes de correo mal dirigido.
- Capacitar al personal sobre los procedimientos de envío por correo y actualizar la capacitación periódicamente.

LISTA DE VERIFICACIÓN PARA ENVÍO POR FAX

- Verificar cuidadosamente el número de fax antes de enviar.
- Confirmar el número con el destinatario cuando sea la primera vez o no sea un número habitual.
- Programar números utilizados regularmente y verificar que se seleccione el correcto antes de enviar.
- Actualizar números de fax cuando se notifique un cambio y eliminar números obsoletos.
- Ubicar las máquinas de fax en áreas controladas y no dejar información del paciente en la máquina después de enviarla.
- Implementar políticas y procedimientos para actuar rápidamente ante cambios de números y reportes de faxes enviados por error.

- Capacitar al personal sobre el uso adecuado del fax y actualizar la capacitación periódicamente.

E. Formularios relacionados

- Hoja de portada de fax

F. Políticas relacionadas

- 11s – Divulgación de PHI
- Enumerar políticas adicionales relacionadas

G. Referencias

- PRA Line Item: C.35, L.3, L.4
- Enumerar referencias adicionales