HIPAA Privacy Policy

Date

04/06/2026

Created For

Elegant Smiles, LLC

Elegant Smiles, LLC

Privacy Policy

Scope:

This Privacy Policy applies to all workforce members of Elegant Smiles, LLC (referred to herein as "the Practice") as defined by HIPAA.

Purpose:

To establish the Practice's policies and procedures for the uses and disclosures of protected health information that may be made by the Practice and its workforce members, and of patient's rights and the Practice's responsibilities with respect to protected health information.

Policy:

It is the Practice's policy to comply with HIPAA's requirements for the privacy of PHI. Accordingly, all members of the Practice's workforce who have access to PHI must comply with this Privacy Policy. For the purposes of this Policy, workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, trainees, and other persons whose work performance is under the direct control of the Practice, whether or not they are paid by the Practice The term "workforce member" includes all of these types of workers.

No third-party rights are intended to be created by this Policy. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or HITECH the Policy shall be aspirational and shall not be binding upon the Practice. To the extent this Policy is in conflict with the HIPAA Privacy Rule, the HIPAA Privacy Rule shall govern.

Protected Health Information: Protected health information ("PHI") means information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living or deceased.

A. Responsibilities of the Practice as a Covered Entity

1. **Privacy Officer and Contact Person**
   The Practice will appoint a Privacy Officer. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy of PHI, including but not limited to this Privacy Policy. The Privacy Officer will also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of PHI.

   The Privacy Officer is responsible for ensuring that the Practice complies with the provisions of the HIPAA Privacy Rule regarding third-party business associate vendors or subcontractors, including the requirement that a HIPAA-compliant Business Associate Agreement is in place with business associate vendors or subcontractors. The Privacy Officer shall also be responsible for monitoring compliance with the HIPAA Privacy Rule and this Privacy Policy.

2. **Workforce Training**
   It is the policy of the Practice to provide new hire training and ongoing training to ensure workforce members are aware, knowledgeable, and comply with the regulations related to the HIPAA and HITECH Act. The Privacy Officer is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out functions in compliance with HIPAA and HITECH.

   A log will be maintained by the Privacy Officer of all workforce members who have participated in privacy and breach notification training. Failure by a workforce member to participate in training may result in termination of access to the Practice’s systems and tools that create, collect, or process PHI.

Security Management Process

The Practice will establish appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. The Practice has implemented Security Policies and Procedures that prevent, detect, contain, and correct security violations.

4. **Complaints**
   The Privacy Officer is responsible for creating a process for managing complaints about the Practice's privacy procedures and for handling such complaints. A copy of the complaint procedure shall be provided to any patient upon request. The Privacy Officer is responsible for maintaining the documentation sufficient to meet its burden of proof under §164.414(b).

5. **Sanctions for Violations of Privacy Policy**
   Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Practice's discipline policy, up to and including termination.

6. **Mitigation of Inadvertent Disclosures of PHI**
   The Practice shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if an workforce member or business associate vendor or subcontractor becomes aware of an unauthorized use or disclosure of PHI, either by a workforce member or a business associate vendor or subcontractor, the workforce member or business associate vendor or subcontractor must immediately contact the Privacy Officer so that appropriate steps to mitigate harm to the patient can be taken.

7. **No Intimidating or Retaliatory Acts**
   No workforce member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing, and/or opposing any improper practice under HIPAA.

8. **No Waiver of Rights**
   The Practice does not require individuals to waive their rights under HIPAA for the provision of treatment, payment, or eligibility for services.

9. **Documentation**
   The Practice’s privacy policies and procedures shall be documented and maintained for at least six years from the date from the date of its creation, or the date when it last was in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

   The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Practice will maintain such documentation for at least six years.

10. **Workforce Must Comply with the Practice’s Policy and Procedures**
    All members of the Practice’s workforce (described at the beginning of this Policy and

referred to herein as “workforce members”) who have access to PHI must comply with this Policy.

11. **Breach Notification Requirements**

The Practice will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, the Secretary of the U.S. Department of Health and Human Services (HHS), and the media (when required) if the Practice or one of its business associate vendors or subcontractors discovers a breach of unsecured PHI.

The Practice will abide by privacy standards, which preempt state laws whenever HIPAA privacy requirements are contrary to state law with the following exceptions:

- State laws that Department of Health and Human Services (HHS) establishes as required to prevent fraud and abuse, to ensure appropriate regulation of insurance and health plans, and which are necessary for state reporting on health care delivery, and other purposes;
- State laws that relate to controlled substances;
- State laws that are more stringent than HIPAA; or
- Where state law provides for reporting disease, injury, child abuse, birth, death, or for public health initiatives.

These exceptions will remain in effect until:

- Either state law or federal regulation, requirement, or implementation specification materially changes;
- HHS revokes the exception; or
- If the state law is more stringent related to HIPAA, the Covered Entity will follow the state requirement.

12. **Mandatory Disclosures of PHI**

PHI must be disclosed in the following situations:

- The disclosure is to the individual who is the subject of the information;
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

13. **Other Permitted Disclosures of PHI**

PHI may be disclosed in the following situations without the patient's authorization, when specific requirements are satisfied. The requirements include prior approval of the Privacy Officer. Permissible disclosures are:

- About victims of abuse, neglect or domestic violence;
- For treatment purposes;
- For judicial and administrative proceedings;

- For law enforcement purposes;
- For public health activities;
- For health oversight activities;
- About decedents;
- For cadaveric organ-, eye- or tissue-donation purposes;
- For certain limited research purposes;
- To avert a serious threat to health or safety;
- For specialized government functions; and
- That relate to workers' compensation programs.

However, members of the workforce are not permitted to access his or her own PHI or the PHI of his or her family members.

14. **Disclosing PHI for Public Health Release**

Disclosures to Public Health Authorities: Protected health information may be disclosed to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. (***See Public Health Authority Disclosure Request Checklist.***)

Public Health Authority: means a federal, state, or local agency, or any person or entity acting under a grant of authority from such public agency that is responsible for public health matters as part of its official mandate.

Disclosures to Report Child Abuse or Neglect: Protected health information may be disclosed to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

Disclosures Regarding FDA-Regulated Products and Activities: Protected health information may be disclosed to persons responsible for an FDA-regulated product or activity, for purposes related to the quality, safety, or effectiveness of the FDA-regulated product or activity. Such purposes include the following:

- To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
- To track FDA-regulated products;
- To enable product recalls, repairs, or replacement, or look-back activities (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look-back activities); or

- To conduct post marketing surveillance.

Communicable Diseases: To the extent allowed by state law, protected health information may be disclosed to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition. Except in an emergency, it is preferable to notify the appropriate public health authority, which will then be responsible for notifying the person who may have been exposed. ***See Public Health Authority Disclosure Request Checklist***

Minimum Necessary Disclosures: All disclosures made under this policy must be limited to the minimum amount necessary to carry out the purpose of the disclosure.

Logging of Disclosures: All disclosures made for public health activities must be logged in accordance with the separate policy regarding "Accounting of Disclosures."

15. **Using and Disclosing PHI for Marketing**

In general, the Practice will not use or disclose protected health information for marketing purposes without an authorization from the patient.

Marketing: means

- To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service; and
- An arrangement between the Practice and any other entity whereby
    - the Practice sells or otherwise receives indirect or direct remuneration for disclosing PHI to the other entity; and
    - The other entity or its affiliate(s) uses the protected health information to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

As a general matter, if a communication falls within either definition of marketing, the Practice must obtain a written prior Authorization, and the prior Authorization must state whether the marketing involves direct or indirect remuneration to the Practice from a third party.

However, if the marketing communication falls into either of the following categories of communication, prior Authorization is not required:

- The marketing activity occurs in a face-to-face encounter between the Practice and the individual (**a face-to-face encounter is not: telephone, mail, fax or the internet**); or
- The marketing activity involves a promotional gift of nominal value, such as:
    - Free, sample toothpaste or toothbrushes; or

- Free pharmaceutical samples.

The Practice must make reasonable efforts to ensure that patients who decide to opt out of receiving future marketing communications are not sent such communications. The Practice will not make opting out financially or otherwise overly burdensome for the patient.

The Practice will not sell, nor allow anyone else to sell patient's protected health information.

If the Practice receives payment for marketing/communicating treatment options to an individual, The Practice will have its Notice of Privacy Practices state that it may communicate in this way and the communication will tell patients that the Practice is receiving payment in exchange for the communication and will let patients know how to opt out of further similar communications. The Practice will not make opting out financially or otherwise overly burdensome for the patient. The Practice will obtain patient authorizations before using or disclosing patient protected health information.

16. **Using or Disclosing PHI on Social Media**

The Practice will not use or disclose protected health information on social media sites without obtaining written authorization from the patient.

The Practice will not permit its workforce members to use or disclose protected health information on their personal, non-work-related social media. All workforce members who violate this policy on using or disclosing PHI on social media will be subject to disciplinary actions up to and including, termination. The Practice will monitor social media accounts and communications and implement controls that can flag potential HIPAA violations, including making its workforce members aware of this policy on the use or disclosure of protected health information on social media.

The Practice may use or disclose protected health information in the form of patient images or photographs, patient testimonials, and patient first name for the Practice's own marketing purposes only if the Practice obtains the patient's authorization for the use and disclosure of patient protected health information for such purposes.

The Practice will not use or disclose specific identifiers, e.g. full names, dates of birth, treatment information, etc.

Additionally, the Practice will not:

- Permit its workforce members to post gossip about patients;
- Post any information that would permit an individual to be identified;
- Share photographs or images taken inside a healthcare facility in which patients or protected health information is visible; or
- Share photos, videos, or text on social media platforms within a private group.

If the Practice has social media, the Practice will have its Notice of Privacy Practices state that it may use or disclose patient photographs on its social media for its own marketing purposes, and it will let patients know how to opt out of the use or disclosure of their protected health information on social media. the Practice will not make opting out financially or otherwise overly burdensome for the patient. the Practice will obtain patient authorizations before using or disclosing patient protected health information on its social media.

17. **Disclosure of Sensitive Information**
    At no time may a patient's sensitive information, including HIV/Aids, drug and/or alcohol, genetic, mental health, sexually transmitted diseases or family planning be disclosed without the patient's authorization.

18. **Complying With the Minimum-Necessary Standard**
    Minimum Necessary When Disclosing PHI: the Practice shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. All disclosures not discussed in this Policy must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure. For the types of disclosures the Practice make on a routine and recurring basis, it will implement policies and procedures (which may be standard protocols) that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. For all other disclosures, the Practice will develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the intended purpose of the use, disclosure, and request. Additionally, the Practice will review requests for disclosure on an individual basis in accordance with such criteria.

    Minimum Necessary When Requesting PHI: the Practice shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Practice is requested. All requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

19. **Disclosures of PHI to Business Associates**
    Workforce members may disclose PHI to the Practice's business associate vendors or

subcontractors and allow business associate vendors or subcontractors to create or receive PHI on its behalf. However, disclosures to business associate vendors or subcontractors must also be limited to the minimum necessary. Prior to any use or disclosure, the Practice must first obtain written, satisfactory assurances (e.g. business associate agreement) from the business associate vendor or subcontractor that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," workforce members must contact the Privacy Officer and verify that a Business Associate Agreement is in place.

Business Associate is an entity that:

- On behalf of a covered entity, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

20. **Access**

- As a general rule, the Practice will provide individuals with access to their PHI upon request. Certain types of PHI are exceptions to this policy and will not be provided, including:
    - PHI that is not part of the Practice's designated record set;
    - Psychotherapy notes, which are the personal notes of a mental health care provider documenting or analyzing the contents of a counseling session, that are maintained separate from the rest of the patient's medical record; or
    - Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- The Practice may deny a request for access in certain situations, as listed below. If a request involves PHI in one of these categories and other PHI that is not, the patient will be granted access to all other requested PHI to the extent possible (a partial denial).
    - **Unreviewable grounds for denial include the following:**
        - When the PHI requested is not subject to the right to access (listed above);
        - If the Practice has provided health care to an inmate under the direction of a correctional institution, and providing the PHI would jeopardize the health, safety, security, custody, or rehabilitation of the individual, other inmates, or the safety of any officer, employee, or other person at the correctional institution or someone responsible for the transport of the inmate;
        - If the PHI was created or obtained in the course of research that includes

treatment (during a clinical trial, for example) and the individual agreed to the denial of access when consenting to the research (access may be temporarily suspended for as long as the research project is in progress); or

- When the PHI was obtained from someone other than a health care provider, under a promise of confidentiality, and access by the patient would be reasonably likely to reveal the source of the information.

- **Reviewable grounds for denial include the following situations in which a licensed health care provider, in the exercise of professional judgment, has determined that:**
  - The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).
  - The access requested is reasonably likely to cause substantial harm to a person (other than a health care provider) referenced in the PHI.
  - The request for access is made by the individual's personal representative and provision of access to that person is reasonably likely to cause substantial harm to the individual or another person. For example, a record that identifies the patient as a victim of abuse, and names the personal representative as the perpetrator.

- When a request is denied in whole or in part, the patient will be sent a denial notice that includes the following:
  - The basis for the denial;
  - An explanation of the individual's rights to request a review, in applicable;
  - A description of how the individual may make a complaint to the the Practice or the Secretary of DHHS; and
  - If access is denied because the Practice does not maintain the PHI in its designated record set(s), the notice will include any information the Practice has regarding the location of the requested information.

- When the reason for denial is subject to review and the patient requests a review, the Practice will conduct a review to determine whether the standards of this policy were properly applied in the original denial.

- The Practice will not impose unreasonable measures on a patient requesting access that serve as barriers to or unreasonably delay the patient from obtaining access. For example, the Practice may not require an individual who wants a copy of his/her medical record mailed to her home address to physically come to the office to request access

and provide proof of identity in person.

- The Practice will provide the patient with access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed to by the Practice and the patient. If a patient requests a summary of the information and agrees to pay the associated reasonable, cost-based fee, a summary will be provided.

- The Practice will comply with the following timelines in processing requests for access:
    - Within 30 days of the date of the request, the Practice must provide access, request an extension, or issue a notice of denial for information that is maintained onsite.
    - One extension of up to 30 days is permitted for information that is maintained offsite or is not readily accessible.
    - Requests for extension must be in writing, state the reasons for the delay, and the date by which the patient will either be granted access or receive a notice of denial.

- **Procedures for Right of Access:**
    - **Receiving a request for access:**
        - Requests for access must be in writing, be signed by the patient, and must clearly identify the designated recipient, the PHI being requested, and where to the send the PHI.
        - The Practice may require a specific request form be completed, provided the unit's form and protocol regarding use of the form has been approved by the Privacy Officer.
        - Workforce members will direct any request for access to the workforce member(s) designated to review and process such requests.
    - **Reviewing the request for access:**
        - The designated workforce member(s) will review the access request to ensure it meets the requirements under this section and will perform an identity check to verify that the requesting party is the individual to whom the PHI pertains or an authorized personal representative.
        - The designated workforce member(s) will approve or make a recommendation to deny the requested access.
    - **Processing approved requests for access:**
        - The workforce member who is authorized to release PHI in response to an approved request for access will locate the requested PHI and provide it in the requested form or format.
        - The PHI will be provided to the designated recipient, in the manner

requested by the individual (in person, by mail, etc). If the individual has requested the PHI be sent via e-mail, the e-mail address must be clearly written on the request and the individual must have been warned of, and accepted, the risks associated with receiving PHI through unencrypted e-mail.
        - the Practice will not charge more than a flat copying fee of $6.50 per request, unless an alternate fee schedule has been approved by the Privacy Officer and it must be a reasonable, cost-based fee.
    - **Processing denied requests for access:**
        - If the Privacy Officer agrees with a recommendation to deny a request, he or she is responsible for sending the patient a denial notice that includes the required information.
        - When the reason for denial is subject to review and the patient requests a review, a review will be conducted by a member of the Practice*'s management who has not participated in the original decision to deny access, the Privacy Officer, or another approved, designated reviewer.
        - The reviewer will provide written notice to the patient of the final determination.

- **Documentation:** A copy of the request for access will be saved in the patient's record, along with either:
    - documentation of the date and manner the request was fulfilled, or
    - copies of the denial notice, review notice, and all related correspondence.

21. **Amendment**

The Practice recognizes the patient's right to request an amendment of protected health information. The patient may seek changes in the medical record, and the provider, under HIPAA rules, has the countervailing right to accept, deny, or otherwise limit those changes. Accepted amendments will be in the form of supplements to the record that will supersede the original material. Original information will not be removed, altered or expunged from the record.

Requesting an Amendment:

- The patient, or patient's legal representative, must make a request in writing, giving supporting reasons for amendment.
- Such amendment will be documented in the patient's paper chart or EMR.
- The provider must notify the patient of his/her decision within 60 days. Where the provider is not able to meet the 60-day deadline, he/she may have an additional 30 days, but must give the patient a written statement of the reasons for the delay and set a firm time for giving an authoritative answer.

Accepting an Amendment:

- The provider must complete an acceptance form to notify the patient that he/she has decided to accept the amendment.
- The provider should identify any business associates or other persons known to have the information that has been amended, and that relied on this information to the patient's detriment.
- The Practice will forward the acceptance form and amendment to the medical records department or Privacy Officer.
- The Practice will mail the original form to the requester. A copy of the form will be filed in the medical record along with the amendment.
- The amendment acceptance form will request the patient to identify any outside holders of the information who should be notified of the amendment. This completed form will be directed to the Medical Records Department or Privacy Officer.
- The Practice or Privacy Officer, on behalf of the provider, will make reasonable efforts to inform persons identified by the provider and the patient as having received the original information.
- The Practice or Privacy Officer will note on the form all parties notified of the amendment, and will replace the copy with the original, completed form in the patient's medical record.
- The Practice or Privacy Officer will update the appropriate log to reflect steps taken, decisions made, and parties notified.

Denying Request for Amendment:

- The provider may deny the request if:
    - The information was not created by him/her;
    - The information is not available to the patient for inspection or copying;
    - The information is not included in the designated record set; or
    - The information is already accurate and complete.

- If the provider decides to deny the patient's request to amend the records, the provider will give the patient timely written notice of the denial. The denial must include the following elements:
    - The basis for denial (See #1 above);
    - Notice of the patient's right to submit a written statement to the provider disagreeing with the denial, including instructions for filing this statement;
    - A statement that, if he or she does not submit a statement of disagreement, the patient may require the provider to include the patient's request for amendment and the provider's denial with any future disclosure of the information;
    - A description of how the patient may complain of the denial in accordance with the Practice's general HIPAA complaint procedures and to the Federal Department of Health and Human Services;

    - The provider must ensure that the materials that the patient wanted to amend contain the following information:
        - The patient's original request for an amendment;
        - The provider's denial of the request;
        - Any statement of disagreement submitted by the patient;
        - The provider's written rebuttal, if any, to any statement of disagreement from the patient.

- The provider must include all of the above material in any future disclosure of the protected health information in question. Alternatively, the provider can include an "accurate summary" of the information.

Handling Receipt of Amended Information:
Amended information received from another provider or payor will be directed to the Medical Records Department or Privacy Officer where it will be logged in. Such notice will be filed in the patient's paper chart or EMR. Amendment notices received in error will be placed in a confidential container for shredding.

22. **Restrictions**

The Practice recognizes the patient's right to request that they voluntarily agree to restrict use or disclosure of protected health information (PHI) to carry out treatment, payment, or health care operations that would otherwise be permitted by law.

Patients have the right to request restrictions on the information that Covered Entities may release to family or friends.

The Practice will permit patients to request to receive the communications of their protected health information by alternative means, or alternative locations. the Practice will not require an explanation of such a request.

The Practice will accommodate reasonable requests, but are not required to agree to all requests for restrictions.

Restriction Requests:

- Patients will be directed to the Privacy Officer to obtain forms to request restrictions of PHI.
- The nature of the information to be restricted will be determined where the request is routed.
- The Privacy Officer will determine the management personnel to best make a determination, and determinations will be made only by providers or personnel of

manager level or above.

- Requests for alternative communications may be conditioned upon how payment will be handled, or provision of an alternative address or method of contact.
- Special restrictions that are accepted will be implemented promptly, with notification to only those workforce members who are necessary to implement the restrictions.
- The Practice may break the agreement during a medical emergency, if needed. The emergency medical provider will be asked not to further use or disclose the restricted information.
- An agreement to restrict information does not prevent use or disclosures for the following purposes:
    - Certain public health activities;
    - Reporting abuse, neglect, domestic violence or other crimes;
    - Health agency oversight activities or law enforcement investigations;
    - Judicial or administrative proceedings;
    - Identifying decedents to coroners and medical examiners;
    - Organ procurement;
    - Certain research activities;
    - Worker's compensation; or
    - Uses or disclosures otherwise required by law.

- The Practice may terminate such an agreement to special restriction under the following conditions:
    - Patient requests termination by a written, or a documented oral agreement; or
    - The Practice notifies the patient of terminated agreement, effective for only PHI created or received after the notification is received.
- All agreed upon restrictions will be clearly documented in the patient record, and will be retained for a period of not less than six (6) years.

23. **Accounting of Disclosures**

An individual has the right to obtain an accounting and an Access Report of certain access and disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, except for electronic disclosures of Electronic Health Records (EHRs), for which the right to an accounting extends:

- To carry out treatment, payment, or health care operations (except in the case of EHRs, for which this exception does not apply)
- To individuals about their own PHI
- Incident to an otherwise permitted use or disclosure
- Pursuant to an authorization
- To persons involved in the individual's care or payment for the individual's care or for certain other notification purposes
- To correctional institutions or law enforcement when the disclosure was permitted

without authorization

- As part of a limited data set
- For specific national security or law enforcement purposes
- Disclosures that occurred prior to the compliance date

The Practice shall respond to an accounting request within 30 days. If the Practice is unable to provide the accounting within 30 days, the Practice may extend the period by 30 days, provided that the Practice gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

24. **Disclosures of De-Identified Information**

the Practice may freely use and disclose information that has been “de-identified” in accordance with the HIPAA Privacy Rule. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

B. Changes to Policies and Procedures

1. **Changes to Notice of Privacy Practices**

If the Practice changes a privacy practice described in its Notice of Privacy Practices, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if it has included in its notice a statement reserving its right to make such a change in its privacy practices.

The Practice will ensure that the policy and procedure that is revised based on changes to its Notice of Privacy Practices comply with HIPAA, and that the revisions are documented in the policy and procedure to comply with the HIPAA’s documentation standard.

The Practice will promptly revise and distribute its Notice of Privacy Practices whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Please note that except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

The Practice will make its Notice of Privacy Practices available upon request to any person and to individuals as specified and required by HIPAA.

2. **Changes to Other Policies and Procedures**
   The Practice will change is policies and procedures as necessary and appropriate to comply with changes in the law, including HIPAA. the Practice may, at any time, change its policies and procedures, and if the change materially affects the content of its Notice of Privacy Practice, the Practice will follow the above-process to ensure that it complies with the applicable Privacy provisions.

The Practice will document all changes to its policies and procedures prior to the effective date of the change.