Sierra HOPE
POLICIES AND PROCEDURES FOR PATIENT RIGHTS

INTRODUCTION

These policies and procedures address patient rights. Under HIPAA, patients are guaranteed certain rights and protections for their privacy, regarding certain information we maintain about them.

POLICIES AND PROCEDURES

RIGHT TO INSPECT AND COPY

1. Patients have the right to inspect and obtain a copy of their designated record set. A Designated Record Set is simply protected health information records that are used, in whole or in part, to make decisions about patients, their treatment, or billing for services rendered. For many practices, this mainly includes medical and billing records for a patient.

2. Patients wishing to inspect and/or copy their designated record set must submit their request in writing to the Privacy Officer at our mailing address. Patients will be informed in the Notice of Privacy Practices of the requirement that a request for access be in writing.

3. Patients may be denied access for the following reasons:

    a. Access is reasonably likely to endanger the life or physical safety of the patient or another person
    b. The information requested constitutes Psychotherapy notes
    c. The information requested was compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding
    d. The information is subject to (and access is denied under applicable provisions) or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA)
    e. As an inmate, the patient's access can be denied by a correctional institution or us, as a provider acting under the direction of a correctional institution, if such access would jeopardize the health, safety, security, custody or the rehabilitation of the patient or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for the patient's transportation
    f. The information was obtained in the course of research that includes the patient's treatment and access will be denied while research is in progress
    g. The information requested that is also subject to the Privacy Act, 5 U.S.C. 552a.
    h. The requested PHI was obtained from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information

4. This practice will respond within thirty (30) calendar days to any written request for access to PHI.

5. Denials for access will be communicated via a written letter to the address specified by the patient.

6. If access is granted a copy of the patient's requested PHI will be made available for the patient to review or will be mailed to an address designated by the patient.

7. Patients have the right to inspect and obtain a copy of our Notice of Privacy Practices which documents our use and disclosure practices.

8. If Patients request a copy of their PHI, we will charge a reasonable cost-based fee for the costs of copying, mailing or other supplies associated with the request. The fee schedule is based on our costs for copy supplies and labor costs for copying. We currently charge $0._____ per page for copies plus the actual cost of postage for mailing. For faxing documents, we charge $0._____ per page for the cost of fax supplies and telephone line costs.

9. We will notify the patient of the cost involved and the patient may choose to withdraw or modify the request at that time before any costs are incurred.

10. Patients must pay the fee in full before they can obtain a copy of the information; however, patients have a right to inspect their PHI without paying any fee.

11. The Notice of Privacy Practices is required to be provided during the first encounter with the patient.

12. The Notice of Privacy Practices must always be available upon request.

13. The Notice of Privacy Practices will be posted in the place where services are provided.

14. The Notice of Privacy Practices will be placed on this practice's web site (if we have one).

15. When the Notice of Privacy Practices is revised, the revised copy will be posted and available upon request.

RIGHT TO AMEND

1. If the patient feels that the information we have about them in their designated record set is incorrect or incomplete, they may ask us to amend the information. A Designated Record Set is simply protected health information records that are used, in whole or in part, to make decisions about patients, their treatment, or billing for services rendered. For many practices, this mainly includes medical and billing records for a patient.

2. Patients have the right to request an amendment for as long as the information is kept.

3. To request an amendment, the patient request must be made in writing and submitted to the Privacy Officer at our mailing address. The patient should include the reason that supports the request. Patients will be informed in the Notice of Privacy Practices of the requirement that an amendment request be in writing.

4. A written response will be mailed to the patient within sixty (60) calendar days on the disposition of their amendment request. If additional time is needed, this practice will inform the patient within the sixty (60) days in writing of the delay, the reason for the delay, and the date the accounting will be provided that will be no later than 90 days from the original request.

5. If the amendment request is accepted by this practice we will:

    a. Add the amendment to the patients PHI
    b. Inform the patient that the amendment was accepted
    c. Ask the patient in writing to identify entities that should be notified of the amendment
    d. Obtain the patient's permission to contact those entities
    e. This practice will make a reasonable effort to inform entities, including business associates, to whom we have disclosed the information and who could be predicted to use the information to the extent that the patient agrees that we may notify these entities

6. We may deny a patient's request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny a patient's request if they ask to amend information that:

    a. Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
    b. Is not part of the designated record set kept by our office
    c. Is not part of the designated record set which they would be permitted to inspect and copy (see item 2 previous section); or
    d. Is accurate and/or complete
    e. The information constitutes psychotherapy notes

7. If the amendment request is denied by this practice we will:

    a. Provide a written denial notice within sixty (60) calendar days
    b. Permit the individual to submit a written statement disagreeing with the denial and to give the basis for the disagreement
    c. May write a rebuttal to the disagreement and provide a copy of the rebuttal to the patient
    d. Will append the following to the record containing the disputed information:
        - Request for amendment
        - Denial of amendment
        - Statement of disagreement
        - Written rebuttal

8. This practice will include in any subsequent disclosure of the PHI contained in the disputed record:

    a. The request for amendment that was submitted by the patient (or an accurate summary of the request)
    b. The denial of request for amendment
    c. Any statement of disagreement (or an accurate summary of the statement) submitted by the patient
    d. This practice's rebuttal of the statement of disagreement

RIGHT TO AN ACCOUNTING OF DISCLOSURES

1. Patients have the right to request an "accounting of disclosures." This is a list of the disclosures we made of PHI about the patient, that were not made to the patient, pursuant to an authorization by the patient, was not an incidental disclosure or part of a limited data set (data that does not include directly identifiable information), used for research, used for public health purposes, to persons involved in the patient's care, for national security or intelligence purposes, to correctional institutions or law enforcement, for treatment, payment or health care operations, or for disclosures made prior to the date of compliance with privacy standards.

    An incidental use or disclosure is described as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. Such incidental uses or disclosures are not considered a violation of the Privacy Rule provided that the covered entity has met the reasonable safeguards and minimum necessary requirements. For example, if these requirements are met, doctors' offices may use waiting room sign-in sheets, hospitals may keep patient charts at bedside, doctors can talk to patients in semi-private rooms, and doctors can confer at nurse's stations without fear of violating the rule if inadvertently overheard by a passerby.

2. Disclosures and requests for an accounting of disclosures will be tracked in the Log of PHI Disclosures form that will be maintained in the patients file.

3. To request an accounting of disclosures, the patient must submit a request in writing to the Privacy Officer at our mailing address. Patient request must state a time period that may not be longer than six years and may not include dates before April 14, 2003.

4. Patient request should indicate in what form they want the list (for example, on paper, electronically). The first list they request within a 12-month period will be free. We will charge the patient a reasonable cost-based fee for providing any additional lists within a 12 month period. The fee schedule is based on our costs for copy supplies and labor costs for preparation of the accounting. The estimated cost for the second accounting within a 12 month period will be calculated prior to preparing the accounting.

5. We will notify the patient of the cost involved and the patient may choose to withdraw or modify their request at that time before any costs are incurred.

6. Patients must pay the fee in full before they can obtain the requested accounting

7. This practice will respond to requests for accounting disclosures within sixty (60) calendar days.

8. If additional time is needed, this practice will inform the patient within the sixty (60) days in writing of the delay, the reason for the delay, and the date the accounting will be provided that will be no later than 90 days from the original request.

RIGHT TO REQUEST RESTRICTIONS

1. Patients have the right to request a restriction or limitation on the PHI we may use or disclose about them for treatment, payment or health care operations. They also have the right to request a limit on the PHI we disclose about them to someone who is involved in their care or the payment for their care.

2. We are not required to agree to the patient's request. If we do agree, we will comply with the request unless the information is needed to provide the patient emergency treatment.

3. To request restrictions, the patient must make their request in writing to the Privacy Officer at our mailing address.

4. Each request must state the following:

    a. What information the patient wants to limit
    b. Whether the patient wants to limit our use, disclosure or both
    c. To whom the patient wants the limits to apply

5. If the Privacy Officer agrees to the restrictions, the request with an approval stamp will be attached to the front of the patient's file to allow anyone using or disclosing the patient's PHI to see the restrictions.

6. The Privacy Officer is authorized to agree to such restrictions on the practice's behalf.

7. This practice may terminate its agreement to restrict the uses and disclosures of an individual's information under the following conditions:

    a. If the individual agrees to or requests the termination in writing;
    b. If the individual orally agrees to the termination and the oral agreement is documented;
    c. If the covered entity informs the individual that it is terminating the agreement, but the termination is only effective with respect to PHI created or received after the termination notification date.

8. In the event this practice believes that a use or disclosure of restricted PHI is necessary for emergency treatment, the covered entity may use or disclose the PHI to provide such treatment. If PHI is disclosed to a health care provider for emergency treatment, the practice will request that the health care provider not further disclose the PHI.

9. Any agreement to restrict PHI must be retained for a period of six (6) years from the date of its creation or from the date it was last in effect, whichever is later.

10. There is no requirement that this practice honor any restriction requests made by an individual.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

1. Patients have the right to request that we communicate with them in a certain way or at a certain location.

2. To request confidential communications, patients must make their request in writing to the Privacy Officer.

3. We will not ask the patient the reason for the request.

4. We will accommodate all reasonable requests.

5. Patients must specify how or where they wish to be contacted.

6. The request with an approval stamp will be attached to the front of the patient's file to allow anyone communicating with the patient to see and honor the request for confidential communication.

Sierra HOPE
POLICIES AND PROCEDURES FOR PHI USE AND DISCLOSURES

INTRODUCTION

These policies and procedures address handling, safeguarding, using, and disclosing protected health information (PHI). Under HIPAA, covered entities must ensure the privacy of a patients' protected health information.

PHI refers to all information (oral, paper-based documents, and electronic documents) that relates to an individual including but not limited to:

- Medical information
- Billing information
- Financial information
- Names and other identifying information such as:
    - Telephone numbers
    - Fax numbers
    - Electronic Mail addresses
    - Social security numbers
    - Medical record numbers
    - Birth date
    - Date of death
    - Health plan beneficiary numbers
    - Account numbers
    - Certificate/license numbers
    - Vehicle identifiers and serial number, including license plate numbers
    - Device identifiers and serial numbers
    - Full face photographic images and any comparable images
    - Any other unique identifying number characteristic, or code

POLICIES AND PROCEDURES

MINIMUM NECESSARY

1. When using or disclosing protected health information, we will take reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. The following are situations in which the Minimum Necessary provisions would **not** apply:

    - Uses or Disclosures that are required by law
    - Uses or Disclosures made to the individual
    - Uses or Disclosures made pursuant to an authorization
    - Disclosures to a health care provider for treatment purposes
    - Disclosures to the Secretary of Health and Human Services for enforcement purposes
    - Uses or Disclosures that are required for compliance with HIPAA requirements

3. Before using or disclosing information consider two basic questions:

    a. How much information is needed to fulfill the purpose of this request?
    b. Are we about to provide information that is not necessary to fulfill the purpose of this request?

    For example: When an insurance company requests documentation that the patient was treated for a broken arm, it is not necessary to provide information about the patient's treatment for high blood pressure.

TREATMENT

1. PHI may be used by or disclosed to the appropriate health care providers to provide patients with medical treatment or services.

2. The identity of any person contacting this practice requesting protected health information (PHI) must be verified before any disclosure may take place.

3. Staff members must also verify the requesting person's authority to have access to the PHI.

4. In cases where a public official is requesting PHI, you must verify the identity of the requester by examining reasonable evidence, such as a written statement of identity on agency letterhead, an identification badge or similar proof of status. In addition, the legal authority must be determined and verified by examining the reasonable evidence, i.e., a written request provided on agency letterhead that describes the legal authority for requesting the release.

PAYMENT

1. PHI may be used or disclosed so that the treatment and services patients receive may be billed and payment may be collected from the patient, an insurance company or a third party.

2. PHI may be used or disclosed to obtain prior approval or to determine whether a patient's insurance will cover the treatment.

HEALTHCARE PURPOSES

1. PHI may be used or disclosed to appropriate personnel in reviewing treatment and services and in evaluating the performance of staff in caring for patients.

APPOINTMENT REMINDERS

1. The minimum necessary medical information may be used to contact patients as a reminder that they have an appointment for treatment or medical care.

2. If a patient makes a reasonable request for an appointment reminder via an alternative method of notification (such as e-mail), the medical staff will honor such a request.

TREATMENT ALTERNATIVES

1. The minimum necessary medical information may be used and disclosed by our organization to tell patients about or recommend possible treatment options or alternatives that may be of interest to them.

HEALTH RELATED BENEFITS AND SERVICES

1. The minimum necessary PHI may be used and disclosed to tell patients about health-related benefits or services that may be of interest to them, such as treatment options and this practice's own health-related products and services.

AS REQUIRED BY LAW

1. We will disclose PHI about patients when required to do so by federal, state or local law.

TO AVERT A SERIOUS THREAT TO HEALTH OR SAFETY

1. We may use and disclose PHI about patients when necessary to prevent a serious threat to the patient's health and safety or the health and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

LAWSUITS AND DISPUTES

1. PHI may be disclosed in response to a subpoena, discovery request, or other lawful order from a court.

AS PERMITTED BY LAW

1. To the extent that the law permits us to release information, we may disclose PHI if asked to do so by a law enforcement official as part of law enforcement activities; in investigations of criminal conduct or of victims of crime; in response to court orders; in emergency circumstances.

Sierra HOPE
POLICIES AND PROCEDURES FOR BUSINESS ASSOCIATES

INTRODUCTION

These policies and procedures address interactions with Business Associates. A Business Associate is considered to be a person or organization that performs a function or activity involving the use or disclosure of PHI on behalf of a covered entity, but is not part of the covered entity's workforce. A Business Associate can also be a covered entity in its own right. Business Associates can be but are not limited to the following:

- Claims processors or administrators
- Billing Agencies
- Benefit managers
- Consultants
- Clearing houses
- Storage Facilities
- Lawyers
- Accountants
- Collection Agencies
- Medical Answering Services
- Temporary Staffing Agencies

Business Associates are involved in the use or disclosure of protected health information while performing a function on behalf of a covered entity and are expected to adhere to the same standards for safeguarding PHI as the covered entity as to protected health information. Under HIPAA, the Department of Health and Human Services has no direct jurisdiction over Business Associates. Covered entities are expected to assure that PHI is used and disclosed appropriately by:

- Entering into Business Associate Contracts to protect the privacy of PHI
- Investigating when complaints or other credible evidence of violations by a Business Associate are received.
- Taking reasonable steps to correct a breach or terminate the contract with a Business Associate after becoming aware of a material breach by a Business Associate.

POLICIES AND PROCEDURES

1. We will obtain satisfactory assurances that the Business Associate will appropriately safeguard any protected health information entrusted to it.

2. The Business Associate will sign an agreement stating that it will not use or disclose protected health information in any manner which would not be permissible for the covered entity under the HIPAA privacy regulations.

3. Business Associates will:

    a. Not use or further disclose protected health information other than as permitted under the contract or as required by law
    b. Use appropriate safeguards to prevent use or disclosure of protected health information other than provided by the contract
    c. Report to our Privacy Officer any violation of use or disclosure as stated in the contract
    d. Ensure that any agents to whom it provides protected health information agree to the same restrictions
    e. Provide a list of agents with their contact information that have been granted access to protected health information to our Privacy Officer
    f. Provide proof that it's employees and agents have been trained in protecting health information

4. All reported and/or discovered violations of the Business Associate contract will be recorded and maintained in a file with the signed contract.

5. If this organization becomes aware of a pattern or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under its contract, this organization will take actions (discussions with the Business Associate, sanctions, and etc.) to cure the breach or to end the violation. If such steps are not successful this organization will terminate the contract if feasible. If it is not feasible to terminate the contract we will report the problem to the Department of Health and Human Services.

Sierra HOPE
POLICIES AND PROCEDURES FOR COMPUTER SYSTEMS

INTRODUCTION

This section describes the set of policies and procedures around usage of computer and communication systems. While these policies and procedures may make good privacy practices, they are not designed to assure that we are in compliance with the Security Standards. The organization will need to review its systems and implement needed changes in accordance with the final Security Standards prior to the compliance date for the standards.

POLICIES AND PROCEDURES

PASSWORDS

1. All systems will require a valid user ID and password

2. Passwords will have the following characteristics:

    a. Passwords will be at least six characters long
    b. All user-chosen passwords should have at least two alpha (letter) and two numeric (number)
    c. The use of control characters and non-printing characters is prohibited

3. It is recommended that all users change their passwords at least every six months

4. In the event of a suspected or actual password breach those passwords are to be changed immediately

5. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator

6. The display or printing of passwords will be masked so that unauthorized parties will not be able to observe or recover them

7. Passwords will not be stored in written or readable form

8. Upon termination all passwords for the employee will be immediately changed or deactivated

ACCESS

1. Computer screens will be positioned in such a manner that only authorized users may see the information contained on the screen

2. All terminals will have a password protected screen saver that will be activated after ten minutes of inactivity

3. If computer equipment will be permanently taken out of service, the hard drive will be totally erased

4. Install Antivirus software

5. Update Antivirus software every six months

6. Automatic logoff of systems after 30 min of inactivity

7. A notice, at system start-up, warning that only those with proper authority should access the system will be displayed initially before signing onto the system OR a written notice with a warning that only those with proper authority should access the system will be displayed near the computer terminal

8. Individuals who are not employees, contractors, consultants, or business partners will not be granted access to any systems

9. Employees will logoff the system before going to lunch or taking breaks

10. Employees will logoff the system before they end their shift for the day

11. The room where the workstation is contained will be locked when not in use

12. All removable media (e.g. CD-ROMs. backup tapes, diskettes, and etc.) will be stored in a locked cabinet to prevent unauthorized use

13. All removable media (e.g. CD-ROMs backup tapes, diskettes, etc.) no longer in use will be reformatted or destroyed preventing any protected health information from being seen by unauthorized individuals

14. Printed versions (hardcopy) of protected health information will be shredded before it is discarded

15. System access will be reviewed annually to remove identification codes and passwords of users who no longer require access

REMOTE ACCESS

1. Remote access via modem should be through an approved security mechanism such as a dial back system, or only allowing modem connectivity from specified phone numbers

2. After three unsuccessful attempts to enter a password, the involved user ID will be suspended until reset by the system administrator

INTERNET

1. Use of the Internet via our network will be primarily for business or professional development

2. Use of the Internet via our network is not permitted for personal use

3. A firewall will be installed to protect against unauthorized intrusion

E-MAIL (ELECTRONIC MAIL)

1. Prohibited use of the electronic mail system includes, but is not limited to:
    a. Disclosure of an individuals personal health information without appropriate authorization
    b. Transmission of information inside or outside of the organization without a legitimate business need for the information
    c. Use for marketing purposes without explicit permission of the patient

2. Patients will be informed about privacy issues such as:
    a. Who besides addressee processes messages
        i. During addressee's usual business hours.
        ii. During addressee's vacation or illness.
    b. That messages are to be included as part of the medical record.

3. The following types of transactions (prescription refill, appointment scheduling, etc.) and sensitive subject matter (HIV, mental health, etc.) should not be sent over e-mail.

4. Patients will be instructed to put category of transaction in subject line of message for filtering: "prescription," "appointment," "medical advice," "billing question."

5. Patients will be instructed to put their name and patient identification number in the body of the message.

6. All messages will be printed, with replies and confirmation of receipt, and placed in patient's paper chart.

7. We will send a new message to inform the patient of completion of request.

8. The sharing of company e-mail accounts with family members is strictly prohibited.

9. We will double-check all "To:" fields prior to sending messages.

10. We will perform at least weekly backups of mail onto long-term storage

11. The use of distribution lists for distributing confidential information is strictly prohibited

12. The subject line will contain a notation referring to the confidential or sensitive nature of the information

13. Document patient consent to guidelines for e-mail use:

    a. E-mail will not be used for emergencies or time-sensitive issues
    b. Privacy and security of e-mail messages is not guaranteed
    c. Staff other than the physician may read and process e-mail
    d. Indemnify our organization for information loss due to technical failures

14. Patient authorization should be obtained before forwarding protected health information to a third party such as a consultant or health plan

15. Patient e-mail addresses will not be supplied to third parties for advertising or any other use

16. When an e-mail account will not be monitored during a vacation or office closure, an auto reply should be sent notifying the sender that the intended recipient is away

17. Upon termination of employment the e-mail account will be deactivated

BACKUP AND RECOVERY

1. A full system backup to tape will be performed every Friday

2. A incremental backup will be performed Monday, Tuesday, Wednesday, and Thursday

3. After being used for 6 months the tape will be destroyed and discarded; and replaced by a new tape

4. Backup tapes will be stored off-site in a secure location

5. Backup and recovery procedures will be tested a least once a year

Sierra HOPE
POLICIES AND PROCEDURES FOR FACSIMILE MACHINE

INTRODUCTION

This section describes the set of policies and procedures around usage of the facsimile (fax) machine.

POLICIES AND PROCEDURES

GENERAL RULES FOR FACSIMILE USE

1. Facsimile machines will be kept in secure areas where members of the workforce that do not require routine access to PHI and patients do not have ready access

2. Use of our facsimile machine(s) is not permitted for personal use

PROCEDURES FOR SENDING FACSIMILES

1. Prior to sending the initial facsimile to an entity, we will verify the facsimile phone number and we will call the recipient before sending the facsimile to let them know it is about to be transmitted.

2. A cover letter should precede each facsimile transmission with the following information:

    a. Date and time of transmission
    b. Sending facility's name, address, telephone number and facsimile number
    c. Name of person sending the facsimile
    d. Authorized receivers name
    e. Number of pages transmitted
    f. Confidentiality statement, with directions on disclosure and destruction

3. If a facsimile does not reach its intended destination:

    a. Note in a log
    b. Send a facsimile to that number explaining that the transmission information was misdirected and ask that the documents be returned by US mail
    c. Call intended recipient and verify facsimile information
    d. Notify Privacy officer

4. Any facsimile containing protected health information will be stored in a secured area where patients and members of the workforce that do not require routine access to PHI will not have ready access

5. Any facsimile document containing protected health information will be shredded before it is discarded

PROCEDURES FOR RECEIVING FACSIMILES

1. When receiving a facsimile transmission:

    a. Remove documents promptly and deliver to intended recipient
    b. Follow instructions on cover page
    c. Notify sender of any transmission problems
    d. Notify the sender of any misdirected documents and either return by mail or destroy depending on the request of the sender

2. Any facsimile document containing protected health information will be shredded before it is discarded

Sierra HOPE
POLICIES AND PROCEDURES FOR WORKFORCE TERMINATIONS

INTRODUCTION

These policies and procedures address handling the privacy and security issues when an employee (or other member of the workforce) leaves the organization or is terminated.

POLICIES AND PROCEDURES

1. When an individual will no longer be a member of the organization, both physical and electronic access to information will be denied
2. New combinations to combination locks will be issued; if a new combination cannot be issued then the combination lock will be changed
3. Security system access codes will be changed immediately
4. Security will be notified that the individual leaving the organization is no longer granted access under any conditions
5. All office staff will be notified that the individual leaving the organization is no longer granted access (keys, combinations, passwords, and etc.) under any conditions
6. The individual leaving the organization will be removed from all access lists
7. The individual leaving the organization will turn in their keys, tokens, or cards that allow access to their supervisor or the security officer as part of terms of receiving their final paycheck
8. All user accounts of the individual leaving the organization will be terminated
9. Any partners or entities that have access to protected health information will be notified to deny the terminated individual access

Sierra HOPE
POLICIES AND PROCEDURES FOR WORKFORCE TRAINING

INTRODUCTION

These policies and procedures address workforce training in privacy and security. The workforce consists of but is not limited to the following: employees, volunteers, students, trainees, and affiliates

POLICIES AND PROCEDURES

1. All current members of the workforce who are likely to come into contact with protected health information will be trained in this practice's policies and procedures with respect to protected health information.

2. New members of the workforce will receive training within sixty (60) days of beginning their affiliation with this practice.

3. If there is a material change in the practice's privacy policies and procedures, all members of the workforce whose duties are directly affected by the change will be retrained within sixty (60) days.

4. Upon completion of training, members of the workforce will be required to sign the confidentiality agreement certifying that he or she received the privacy training and will honor this practice's privacy policies and procedures.

5. Each member will sign a new confidentiality agreement within three (3) years of the date they last signed this practice's confidentiality agreement.