

Erika M. Steffe MD
Infectious Diseases/Northern California Travel Clinic
Integrative Medicine
1131 Gravenstein Highway South
Sebastopol, CA 95472
Phone: 707 823-3877 FAX: 707/823-3851

PRIVACY POLICY STATEMENT

Purpose: The following privacy policy is adopted to ensure that this Physician Practice complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of paramount importance to this organization. Violations of any of these provisions will result in severe disciplinary action including termination of employment and possible referral for criminal prosecution.

Effective Date: This policy is in effect as of [effective date].

It is the policy of this Physician Practice that we will adopt, maintain and comply with our Notice of Privacy Practices, which shall be consistent with HIPAA and California law.

Notice of Privacy Practices

It is the policy of this Physician Practice that a notice of privacy practices must be published, that this notice be provided to all subject individuals at the first patient encounter if possible, and that all uses and disclosures of protected health information be done in accord with this organization's notice of privacy practices. It is the policy of this Physician Practice to post the most current notice of privacy practices in our "waiting room" area, and to have copies available for distribution at our reception desk.

Assigning Privacy and Security Responsibilities

It is the policy of this Physician Practice that specific individuals within our workforce are assigned the responsibility of implementing and maintaining the HIPAA Privacy and Security Rules' requirements. Furthermore, it is the policy of this Physician Practice that these individuals will be provided sufficient resources and authority to fulfill their responsibilities. At a minimum it is the policy of this Physician Practice that there will be one individual or job description designated as the Privacy Official.

Deceased Individuals

It is the policy of this Physician Practice that privacy protections extend to information concerning deceased individuals.

Minimum Necessary Use and Disclosure of Protected Health Information

It is the policy of this Physician Practice that for all routine and recurring uses and disclosures of protected health information (PHI) (except for uses or disclosures made 1) for treatment purposes, 2) to or as authorized by the patient or 3) as required by law for HIPAA compliance) such uses and disclosures of PHI must be limited to the minimum amount of information needed to accomplish the purpose of the use or disclosure. It is also the policy of this Physician Practice that non-routine uses and disclosures will be handled pursuant to established criteria. It is also the policy of this organization that all requests for PHI (except as specified above) must be limited to the minimum amount of information needed to accomplish the purpose of the request, and where practicable, to the limited data set.

Marketing Activities

It is the policy of this Physician Practice that any uses or disclosures of protected health information for marketing activities will be done only after a valid authorization is in effect except as permitted by law. It is

the policy of this organization to consider any communication intended to induce the purchase or use of a product or service where an arrangement exists with a third party for such inducement in exchange for direct or indirect remuneration, or where this organization encourages purchase or use of a product or service directly to patients to constitute "marketing". This organization does not consider the communication of alternate forms of treatment, or the use of products and services in treatment, or a face-to-face communication made by us to the patient, or a promotional gift of nominal value given to the patient to be marketing, unless direct or indirect remuneration is received from a third party. Similarly, this organization does not consider communication to our patients who are health plan enrollees in conjunction with our provision, coordination, or management of their health care and related services, including our coordination or management of their health care with a third party, our consultation with other health care providers relating to their care, or if we refer them for health care to be marketing, but only to the extent these communications describe: 1) a provider's participation in the health plan's network, 2) the extent of their covered benefits, or 3) concerning the availability of more cost-effective pharmaceuticals. This organization may make remunerated communications tailored to individual patients with chronic and seriously debilitating or life-threatening conditions provided we are making the communication in conjunction with our provision, coordination, or management of their health care and related services, including our coordination or management of their health care with a third party, our consultation with other health care providers relating to their care, or if we refer them for health care. If we makes these types of communications to patients who have a chronic and seriously debilitating or life-threatening condition, we will disclose in at least 14-point type the fact that the communication is remunerated, the name of the party remunerating us, and the fact the patient may opt out of future remunerated communications by calling a toll-free number. This organization will stop any further remunerated communications within 30 days of receiving an opt-out request.

Mental Health Records

It is the policy of this Physician Practice to require an authorization for any use or disclosure of psychotherapy notes, as defined in the HIPAA regulations, except for treatment, payment or health care operations as follows:

- A. Use by originator for treatment;
- B. Use for training physicians or other mental health professionals as authorized by the regulations;
- C. Use or disclosure in defense of a legal action brought by the individual whose records are at issue; and
- D. Use or disclosures as required by law, or as authorized by law to enable health oversight agencies to oversee the originator of the psychotherapy notes.

Complaints

It is the policy of this Physician Practice that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. Furthermore, it is the policy of this Physician Practice that all complaints will be addressed to [name or job title of person authorized to handle complaints] [(i.e. Privacy Official)] who is duly authorized to investigate complaints and implement resolutions if the complaint stems from a valid area of non-compliance with the HIPAA Privacy or Security Rule.

Prohibited Activities-No Retaliation or Intimidation

It is the policy of this Physician Practice that no employee or contractor may engage in any intimidating or retaliatory acts against persons who file complaints or otherwise exercise their rights under HIPAA

regulations. It is also the policy of this organization that no employee or contractor may condition treatment,

payment, enrollment or eligibility for benefits on the provision of an authorization to disclose protected health information except as expressly authorized under the regulations.

Responsibility

It is the policy of this Physician Practice that the responsibility for designing and implementing procedures to implement this policy lies with the Privacy Official.

Verification of Identity

It is the policy of this Physician Practice that the identity of all persons who request access to protected health information be verified before such access is granted.

Mitigation

It is the policy of this Physician Practice that the effects of any unauthorized use or disclosure of protected health information be mitigated to the extent possible.

Safeguards

It is the policy of this Physician Practice that appropriate safeguards will be in place to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the HIPAA Privacy Rule. These safeguards will include physical protection of premises and PHI, technical protection of PHI maintained electronically and administrative protection of PHI. These safeguards will extend to the oral communication of PHI. These safeguards will extend to PHI that is removed from this organization.

Business Associates

It is the policy of this Physician Practice that business associates must comply with the HIPAA Privacy and Security Rules to the same extent as this Physician Practice, and that they be contractually bound to protect health information to the same degree as set forth in this policy pursuant to a written business associate agreement. It is also the policy of this organization that business associates who violate their agreement will be dealt with first by an attempt to correct the problem, and if that fails by termination of the agreement and discontinuation of services by the business associate, or if that is not feasible, by notification of the HHS Secretary. Finally, it is the policy of this organization that organizations that transmit PHI to this Physician Practice or any of its business associates and require access on a routine basis to such PHI, including a Health Information Exchange Organization, a Regional Health Information Organization, or an E-prescribing Gateway, and Personal Health Record vendors, shall be business associates of this Physician Practice.

Training and Awareness

It is the policy of this Physician Practice that all members of our workforce have been trained by the compliance date on the policies and procedures governing protected health information and how this Physician Practice complies with the HIPAA Privacy and Security Rules. It is also the policy of this Physician Practice that new members of our workforce receive training on these matters within a reasonable time (you may elect to enter the exact time frame) after they have joined the workforce. It is the policy of this Physician Practice to provide training should any policy or procedure related to the HIPAA Privacy and Security Rule materially change. This training will be provided within a reasonable time (you may elect to enter the exact time frame) after the policy or procedure materially changes. Furthermore, it is

the policy of this Physician Practice that training will be documented indicating participants, date and subject matter.

Material Change

It is the policy of this Physician Practice that the term "material change" for the purposes of these policies is any change in our HIPAA compliance activities.

Sanctions

It is the policy of this Physician Practice that sanctions will be in effect for any member of the workforce who intentionally or unintentionally violates any of these policies or any procedures related to the fulfillment of these policies. Such sanctions will be recorded in the individual's personnel file.

Retention of Records

It is the policy of this Physician Practice that the HIPAA Privacy and Security Rules' records retention requirement of six years will be strictly adhered to. All records designated by HIPAA in this retention requirement will be maintained in a manner that allows for access within a reasonable period of time. This records retention time requirement may be extended at this organization's discretion to meet with other governmental regulations or those requirements imposed by our professional liability carrier.

Regulatory Currency

It is the policy of this Physician Practice to remain current in our compliance program with HIPAA regulations.

Cooperation with Privacy Oversight Authorities

It is the policy of this Physician Practice that oversight agencies such as the Office for Civil Rights of the Department of Health and Human Services be given full support and cooperation in their efforts to ensure the protection of health information within this organization. It is also the policy of this organization that all personnel must cooperate fully with all privacy and security compliance reviews and investigations.

Investigation and Enforcement

It is the policy of this Physician Practice that in addition to cooperation with Privacy Oversight Authorities, this Physician Practice will follow procedures to ensure that investigations are supported internally and that members of our workforce will not be retaliated against for cooperation with any authority. It is our policy to attempt to resolve all investigations and avoid any penalty phase if at all possible.