HIPAA Privacy and Security Policy and Procedure

Purpose: To ensure the privacy of protected health information (PHI) from intentional and/or inadvertent disclosure.

Last Review Date: October 22, 2024

Approved By: Manmohan Nayyar MD, President, Rahul Nayyar, MD, CMO, Tammi Castro, VP of Operations

Content

I. **Policy regarding the role and responsibility of the HIPAA Privacy/Security Officer:**

a. The HIPAA Privacy/Security Officer has authority to establish, implement, and enforce these policies and procedures for the security and privacy of our patients protected health information (PHI).

b. The HIPAA Privacy/Security Officer is responsible for conducting an annual HIPAA privacy and security risk assessment. The assessment will be completed with the assistance of at least one other employee. Additional risk assessments may be necessary each time

- new software or hardware is acquired and placed in service
- when a new service or procedure is initiated
- when there is a significant change in an existing service or procedure
- when there is a change or addition to the physical layout of an office

c. The HIPAA Officer will periodically but at least quarterly review the DHHS's HIPAA website to determine if there have been any changes in the HIPAA rules and regulations and to determine if any changes or modifications to this policy and procedure is necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

II. **Policy regarding employee access:** Employee access to administration and/or medical office buildings are restricted to company business hours. Only office managers are provided keys and are responsible for unlocking employee and patient access doors as well as securing all access areas at the end of business. Under the approval of the Administrator, additional employees and/or contractors may be provided access outside of business hours.

III. **Policy regarding confidentiality of all forms of PHI:** All PHI regardless of its form, mechanism of transmission, or storage is to be kept confidential. Only individuals with a business need to know are allowed to view, read, or discuss any part of a patient's PHI. During initial new hire orientation and/or HIPAA training employees are reminded that any viewing, reading, or discussions of PHI that is not for business purposes is prohibited. An employee who violates this confidentiality policy will be subject to sanctions up to immediate termination. All employees are required to verify in writing by signing the HIPAA Compliance Agreement that they will comply with our policy regarding confidentiality of all forms of PHI. Under no circumstance, are employees permitted to view or edit their own account information, including that of family members. Employees who are also members of the medical group are required to follow the same processes, rules and guidelines of patients. Any conflicts that arise within the medical group should be reported to a supervisor immediately.

IV. **Policy regarding Security of electronic PHI (e-PHI)** Employees whose job functions require access to our computer system will be given a secure, unique password to access the system. Access will be immediately terminated for employees who leave our employment. All PHI transmitted to third parties will be transmitted on secured lines. The security of transmission lines will be verified and no digitally stored PHI shall leave this facility without being first encrypted; this includes laptops, flash drive devices, CDs, and e-mail.

V. **HIPAA Incident/Breach Investigation:** Any incident in which the privacy/security of a patient's PHI may have been compromised will be immediately reported to the company's HIPAA Privacy/Security Officer and/or Human Resources. An incident investigation will be initiated without unreasonable delay.

VI. **Sanction Policy:** All employees will receive training regarding company policy for sanctioning employees who violate our HIPAA privacy/security policy. Employees shall receive training prior to assuming work duties and annually thereafter.

VII. **Document Retention Policy:**

a. All HIPAA documentation such as policy and procedures, risk assessment, incident investigation, breach notification, and training records will be maintained for at least six years.

HIPAA COMPLIANCE AGREEMENT

Employees and partners of the practice will have access to confidential information, both written and oral during the course of their employment/contract. In order to ensure the privacy of protected health information
(PHI) from intentional and/or inadvertent disclosure it is imperative that this information is not disclosed to any
unauthorized individuals. An unauthorized individual would be any person that is not currently an employee of
the practice and/or an individual without a ***business need to know***.
All PHI regardless of its form, mechanism of transmission, or storage is to be kept confidential. Only individuals
with a "business need to know" are allowed to view, edit, or discuss any part of a patient's PHI. Under no circumstance, are employees permitted to view or edit their own account information in the company's electronic health record (EHR), including that of family members.
I have read and understand the practice's policy with regards to privacy of PHI. I agree to maintain confidentiality of all information obtained in the course of my employment including, but not limited to, financial,
technical, or propriety information of the organization and personal and sensitive information regarding patients, employees, and vendors. I understand that inappropriate disclosure, release of, or access to PHI is grounds for termination.

Signed: Date:

_____ _____

Print Name:

_____