

Esguerra Dental Implant Associates of Duluth, PLLC
Dental Implant and Reconstructive Center

HIPAA PRIVACY & SECURITY POLICY

I. ASSIGNMENT OF HIPAA PRIVACY/SECURITY OFFICER

Roxanna Esguerra, DDS has been designated as the HIPAA Officer for Esguerra Dental Implant Associates of Duluth, PLLC (the “Company”), and has authority to establish, implement, and enforce these policies and procedures for the security and privacy of patients’ protected health information (“PHI”). The HIPAA Officer may amend this policy from time to time, at the HIPAA Officer’s discretion.

II. RISK ASSESSMENT

The HIPAA Officer is responsible for conducting HIPAA Privacy & Security risk assessment. The HIPAA Officer may periodically, but at least annually, consult with legal counsel 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 are necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

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 at all subsequent HIPAA trainings employees are reminded that any viewing, reading, or discussions of PHI that is not for business purposes is prohibited. All employees are required to verify in writing that they have read and will comply with our policy regarding confidentiality of all forms of PHI.

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. Passwords will consist of at least eight characters, upper and lower case, alpha numeric and shall be changed on a periodic basis.

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 with third parties responsible for transmitting our patient’s PHI.

No digitally stored PHI shall leave any facility without being encrypted; this includes

laptops, flash drive devices, CDs, and e-mail.

V. PATIENT REQUEST FOR ACCOUNTING OF ALL DISCLOSURES MADE BY THE COMPANY

Patients have a right to request an accounting of all disclosures of their PHI. When a patient makes such a request, the Company will comply with applicable law.

VI. PATIENT REQUEST FOR RESTRICTION OF PHI PAID FOR “OUT OF POCKET”

Patients who pay for a procedure, test, or service out of pocket (fully paid for by patient with no reimbursement or additional payment by a third party), have a right to have all information regarding such procedure/test held confidentially and not released to third parties. To exercise this right the patient must (1) pay for test/procedure and (2) make known their desire to have information regarding the procedure/test held in confidence and not released to third parties. Any employee who receives such a request must immediately inform the Company and the information will be restricted. HIPAA allows for the release of restricted PHI (1) in compliance to a subpoena; (2) in compliance to statutory reporting requirement; or (3) upon receiving an unrestricted, HIPAA compliant authorization for release of medical records from the patient, patient’s legal representative, or executor of deceased patient’s estate.

VII. POLICY REGARDING CHARGES FOR E-COPIES OF MEDICAL RECORDS

The Privacy Rule permits the Covered Entity (a healthcare provider) to impose reasonable, cost-based fees for paper copies.

According to HITECH the covered entity may charge for the labor cost of making the e copy. This does not include the cost for searching the data base to find appropriate medical record(s).

Notwithstanding the foregoing, the Company shall abide by and comply with the Minnesota Health Records Act with respect to charging patients for copies of their records.

VIII. BUSINESS CONTINUITY

The Company will develop and implement a business continuation plan, and such plan shall become a part of this Policy.

IX. 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 HIPAA Officer. An incident investigation will be initiated without unreasonable delay.

X. SANCTION POLICY

All employees will receive training regarding policy for sanctioning employees who violate this policy.

XI. DOCUMENT RETENTION POLICY

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.

4827-0513-1734, v. 1