Sample Data Security Policy

Introduction

This Data Security Policy must be understood and followed by all Company employees.

Company data (including data collected or stored relating to clients, customers, patients, employees, etc.) is a valuable Company asset and must be protected. The Company depends on its information systems and, thus, data security is critical.

Data security flows from controlling unauthorized access to data. Breaches in data security poses risk (1) to the Company's ability to service its customers [clients or patients]; (2) of lost revenue through fraud or destruction of proprietary or confidential data; (3) of violation of business contracts, trade secrets, and customer [or patient] privacy; (4) of reduced credibility and reputation with its customers [clients or patients], shareholders and partners.

The goal is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction.

This policy applies to all of our electronic data and all customer electronic data collected, stored or processed by the Company.

This policy will better define the overall objective which is to make all data and data processing resources accessible only on a need to know basis to specifically identified, authenticated, and authorized users or entities. Of course, public data is outside the scope of this policy.

Compliance with this policy is a condition of employment for employees. [Compliance with this policy may also be a contractual agreement for vendors, suppliers, and third party processor or agents, (collectively, "vendors". But, consider the use of a "Data Privacy & Security Agreement" with vendors.] All employees must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Breach of Policy and Enforcement

Violation of this policy will result in disciplinary action up to and including termination. All employees are bound by this policy and are responsible for its enforcement.

Scope of the Policy

This policy applies to all Company and customer data that is collected or stored on any IT Asset owned by the Company, or its employees, or a third party on behalf of the company (sometimes referred to as "covered data"). IT Assets include computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data.

This policy applies to any person or entity that collects or stores covered data related to the Company or its customers [client or patients], current or former employees, and any personal or medical information concerning any person, including full-time or part-time employees, vendors or processors who have access to such data, and other persons, entities, or organizations that have access to such data.

Data Transmission

Employees who access covered data must transmit such data in compliance with this policy. As necessary, communications included covered data must be encrypted during transmission.

Other countries (e.g. the European Union) have different, and often more stringent, privacy laws that apply to information related to individuals ("personal information"). Employees that plan to communicate personal information outside the United States must comply with the laws of the jurisdiction in which recipient of the communication resides.

Data Storage

Employees are responsible for the secure storage of covered data, including customer data, and must do so in compliance with this policy. As necessary, data stored must be secured with encryption. Access control mechanisms must be used to limit access only to authorized users.

Data Disposal

Access control mechanisms must be used to ensure that only authorized users can access covered data during the disposal process. Employees must follow the Company's procedures for the proper disposal of various types of data.

Data Security Policy Statement

This policy is designed to educate Company users [and vendors] about their obligation for protection all covered data; to ensure the security, integrity, and availability of all covered data; and to establish the Company's baseline data security stance and classification system.

Data Security Responsibilities

All managers and supervisors must strive to ensure compliance with this policy by (1) helping each other understand and comply with the requirements herein, and (2) overseeing staff to ensure Company employees understand and comply with the requirements herein.

The Company may establish a Data Security Team that is responsible for:

- Defining the security requirements, controls and mechanisms applicable to all covered data.
- Defining the methods and guidelines used to identify and classify all covered data.
- Defining the procedures for identifying data owners for all covered data.
- Defining the labeling requirements for all covered data.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all Company users [and vendors].
- Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in industry.

Documentation

This policy requires procedures be developed, managed and performed. Thus, written documentation must be developed for all procedures necessary to comply with this policy including:

- The management of all userids and passwords on IT Assets;

- The management of all access control lists on all IT Assets;
- The execution and review of all audit trails;
- All incident response and reporting; and
- All other tasks necessary to support this policy.

Policy Review

This policy should be reviewed on a regular basis because of the dynamic nature of the Internet and data security threats. Accordingly, the Company's CEO [or insert CFO, COO, or other senior management officer] shall determine reasonable schedule for review of this policy and include other senior management, systems administration, and legal counsel in the review process.

Data Classification

Data classification is necessary to enable the allocation of resources to the protection of covered data, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data the default data classification for any covered data is either "Sensitive Personal Information" or "Proprietary Company Data".

The Data Security organization is responsible for evaluating the data classification system and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavors, to develop additional data classifications. All covered data must fall into one of the following categories:

Public Company Data – Public company data is defined as data that any entity either internal or external to the Company can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on the Company nor carry any significant liability. (Examples of Public company data include readily available news, stock quotes, or sporting information.)

Proprietary Company Data – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that the company is under legal or contractual obligation to protect.

The value of Proprietary Company Data to the Company would be destroyed or diminished if such information were disclosed to others. Most of the Company's sensitive information should fall into this category. Proprietary Company Data may be copied and distributed within the Company only to authorized users. Proprietary Company Data disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary Company Data include company policies, sales plans, and application source code.)

Confidential Company Data – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on the Company and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Confidential Company Data must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or cryptographic keys.)

Sensitive Personal Information – Sensitive Personal Information is defined as data that only authorized internal Company entities or specific authorized external entities can access. The disclosure, use, or destruction of Sensitive Personal Information can have adverse affects on the Company and its relationship with its customers, and possibly carry significant liability for both. Sensitive Personal

Information is entrusted to and may transit or is stored by the Company (and others) over which they have custodial responsibility but do not have ownership. (Examples of Sensitive Personal Information include customer bank or brokerage account information, cryptographic keys, or other data considered private.)

Public Customer Data – Public customer data is defined as data that any entity either internal or external to the Company can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on the Company or its customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by the Company (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

Data Ownership— In order to classify data, identify the owner of all covered data. The owner of data is responsible for classifying their data according to the classification system noted in this policy. If an owner cannot be determined for covered data, the Data Security organization must act as its custodian.

The default classification for all data not classified by its owner must be either “Sensitive Personal Information” or “Proprietary Company Data”. The Data Security organization is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

The owner of all Sensitive Personal Information is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer.)

Non-disclosure Agreements

If covered data needs to be released to entities outside of the Company, and a legitimate business reason exists for releasing the information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

I HAVE READ THIS DATA SECURITY POLICY CAREFULLY, AND UNDERSTAND AND ACCEPT THE OBLIGATIONS THAT IT IMPOSES UPON ME, WITHOUT RESERVATION. I UNDERSTAND THAT VIOLATION OF THIS POLICY WILL RESULT IN DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION.

Employee Signature: _____ Date: ___ / ___ / _____

Print Name: _____