IS-2 DATA CLASSIFICATION POLICY

**2.1. Data Classification Policy**

<COMPANY NAME> has procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI) stored in conjunction with <COMPANY NAME> <APPLICATION NAME> customers utilizing our backup service. This policy, and associated procedures for testing and restoring from backup data, do not apply to PaaS Customers that do not choose <COMPANY NAME> Backup Service. The policy and procedures will assure that complete, accurate, retrievable, and tested backups are available for all systems used by <COMPANY NAME>.

Data backup is an important part of the day-to-day operations of <COMPANY NAME>. To protect the confidentiality, integrity, and availability of ePHI, both for <COMPANY NAME> and <COMPANY NAME> Customers, complete backups are done daily to assure that data remains available when needed and in case of a disaster.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.

**2.2 Definitions**

* **Confidential/Restricted Data**: are generalized terms that typically represent data classified as *Sensitive or Private*, according to the data classification scheme defined in this policy.
* **Internal Data**: is defined as all data owned or licensed by <COMPANY NAME>, Inc.
* **Public Information**: is defined as any information that is available within the public domain.

**2.3 Data Classification Scheme**

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to <COMPANY NAME>, Inc. should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All data should be classified into one of the three following classifications.

**Restricted/Confidential Data**

Data should be classified as Restrictive or Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to <COMPANY NAME>, Inc. or its customers. Examples of Sensitive data include data protected by state or federal privacy regulations (e.g. PHI & PII) and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted and Confidential Data.

Disclosure or access to Restricted and Confidential data is limited to specific use by individuals with a legitimate need-to-know. Explicit authorization by the Information Security Officer is required for access to because of legal, contractual, privacy, or other constraints. Restricted/Confidential data:

* Must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure.
* Must be destroyed when no longer needed. Destruction must be in accordance with Company policies and procedures.
* Will require specific methodologies, procedures, and reporting requirements for the response and handling of incidents.

**Internal Use Data**

Data should be classified as Internal Use when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to <COMPANY NAME>, Inc. or its customers. This includes proprietary, ethical, or privacy considerations. Data must be protected from unauthorized access, modification, transmission, storage or other use. This applies even though there may not be a civil statute requiring this protection. Internal Use Data is restricted to personnel who have a legitimate reason to access it. By default, all data that is not explicitly classified as Restricted/Confidential or Public data should be treated as Internal Use data. A reasonable level of security controls should be applied to Internal Use Data.

**Public Data**

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to <COMPANY NAME>, Inc. and its customers. It is further defined as information with no existing local, national, or international legal restrictions on access or usage. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized alteration or destruction of Public Data.

**2.4 Calculating Classification**

The goal of information security, as stated in the Information Security Policy, is to protect the confidentiality, integrity, and availability of Corporate and Customer Data. Data classification reflects the level of impact to <COMPANY NAME>, Inc. if confidentiality, integrity, or availability is compromised. If a classification is not inherently obvious, consider each security objective using the following table as a guide. All data are to be assigned one of the following four sensitivity levels:

|  |  |  |
| --- | --- | --- |
| **CLASSIFICATION** | **DATA CLASSIFICATION DESCRIPTION** | |
| RESTRICTED | Definition | Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need. |
| Potential Impact of Loss | SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to <COMPANY NAME>  Impact could include negatively affecting <COMPANY NAME>’s competitive position, violating regulatory requirements, damaging the company’s reputation, violating contractual requirements, and posing an identity theft risk. |
| CONFIDENTIAL | Definition | Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by <COMPANY NAME>. |
| Potential Impact of Loss | SIGNIFICANT DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to <COMPANY NAME>.  Impact could include negatively affecting <COMPANY NAME>’s competitive position, damaging the company’s reputation, violating contractual requirements, and exposing geographic location of individuals. |
| INTERNAL USE | Definition | Internal Use information is information originating within or owned by <COMPANY NAME>, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company’s business interests. |
| Potential Impact of Loss | MODERATE DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to <COMPANY NAME>.  Impact could include damaging the company’s reputation and violating contractual requirements. |
| PUBLIC | Definition | Public information is information that has been approved for release to  the general public and is freely shareable both internally and externally. |
| Potential Impact of Loss | NO DAMAGE would occur if Public information were to become available to parties either internal or external to <COMPANY NAME>.  Impact would not be damaging or a risk to business operations. |

#### **Handling Controls Per Data Classification**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Handling Controls** | RESTRICTED | CONFIDENTIAL | INTERNAL USE | PUBLIC |
| Non-Disclosure Agreement (NDA) | - NDA is required prior to access by non-<COMPANY NAME> employees. | - NDA is recommended prior to access by non-<COMPANY NAME> employees. | - No NDA  requirements | - No NDA  requirements |
| Internal Network Transmission (wired & wireless) | * Encryption is required * Instant Messaging is prohibited * FTP is prohibited | * Encryption is recommended * Instant Messaging is prohibited * FTP is prohibited | - No special requirements | - No special requirements |
| External Network Transmission (wired & wireless) | * Encryption is required * Instant Messaging is prohibited * FTP is prohibited * Remote access should be used only when necessary and only with VPN and two-factor authorization when   possible | * Encryption is required * Instant Messaging is prohibited   FTP is prohibited | * Encryption is recommended * Instant Messaging is prohibited * FTP is prohibited | - No special requirements |
| Data at Rest (file servers, databases, archives, etc.) | * Encryption is required * Logical access controls are required to limit unauthorized use * Physical access restricted to specific individuals | * Encryption is recommended * Logical access controls are required to limit unauthorized use * Physical access restricted to specific groups | * Encryption is recommended * Logical access controls are required to limit unauthorized use * Physical access restricted to specific groups | * Logical access controls are required to limit unauthorized use * Physical access restricted to specific groups |
| Mobile Devices (iPhone, iPad, USB Drive, etc.) | * Encryption is required * Remote wipe must be enabled, if possible | * Encryption is required * Remote wipe must be enabled, if possible | * Encryption is recommended * Remote wipe should be enabled, if   possible | - No special requirements |
| Email  (with & without attachments) | * Encryption is required * Do not forward | * Encryption is recommended * Do not forward | * Encryption is recommended * Do not forward | - No special requirements |
| Physical Mail | * Mark "Open by Addressee Only" * Use "Certified Mail" and sealed, tamper- resistant envelopes for   external mailings | * Mark "Open by Addressee Only" * Use "Certified Mail" and sealed, tamper- resistant envelopes for external   mailings | * Mail with company interoffice mail * US Mail or other public delivery systems | - No special requirements |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | * Delivery confirmation is required * Hand deliver internally | * Delivery confirmation is required * Hand delivering is recommended over interoffice mail | and sealed tamper- resistant envelopes for external  meetings |  |
| Printer | - Verify destination | - Verify destination printer | - Verify | - No special |
|  | printer | - Attend printer while | destination | requirements |
|  | - Attend printer while | printing | printer |  |
|  | printing |  | - Retrieve |  |
|  |  |  | printed material |  |
|  |  |  | without delay |  |

**Purpose**

This policy will assist employees and other third-parties with understanding the Company’s information labeling and handling guidelines. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect sensitive or confidential information (e.g., Company Confidential information should not be left unattended in conference rooms).

**Scope**

Information covered in this policy includes, but is not limited to, information that is received, stored, processed, or transmitted via any means. This includes electronic, hardcopy, and any other form of information regardless of the media on which it resides.

**Applicable Standards**

Applicable Standards from the HITRUST Common Security Framework

\* 01.v - Information Access Restriction

Applicable Standards from the HIPAA Security Rule

\* 164.308(a)(7)(ii)(A) - Data Backup Plan

\* 164.310(d)(2)(iii) - Accountability

\* 164.310(d)(2)(iv) - Data Backup and Storage

# **Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of changes** |
|  |  | **Initial creation** |
|  |  |  |
|  |  |  |