IS-6 DATA MANAGEMENT POLICY

**6. Data Management 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.

**6.1 Backup Policy and Procedures**

1. Perform daily snapshot backups of all systems that process, store, or transmit ePHI for <COMPANY NAME> Customers.
2. The <COMPANY NAME> Ops Team is designated to be in charge of backups.
3. Dev Ops Team members are trained and assigned to complete backups and manage the backup media.
4. Document backups
	1. Name of the system
	2. Date & time of backup
	3. Where backup stored (or to whom it was provided)
5. Securely encrypt stored backups in a manner that protects them from loss or environmental damage.
6. Test backups annually and document that files have been completely and accurately restored from the backup media.

**Purpose**

The purpose of this procedure is to provide a policy and guideline maintaining the availability of the company’s network and data.

**Scope**

This policy and defined process is used to allow access to ensure the availability of the company’s data and systems. This policy governs individuals who are responsible for maintain information systems in order to support the business. This policy relates to all data used, processed, stored, maintained or transmitted in and through the company’s systems.

**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** |
|  |  |  |
|  |  |  |