**Data Backup Policy**

**Purpose:**

This policy reflects [Insert Covered Entity or Business Associate name] commitment to backup and securely store all ePHI on its information systems and electronic media.

**Scope:**

The IT Department and/or any other department or workforce member that purchases, moves, maintains, and/or creates equipment or media capable of storing or transmitting ePHI.

**Definitions:**

1. Backup: The process of making an electronic copy of data stored in a computer system. Examples of Back-ups Include:
   1. Full/Complete Backup - a backup/image of all data, programs, and files on the system.
   2. Incremental Backup - a backup that only contains the files that have changed since the most recent backup.
   3. Snap-shot Backup (image backup) – a process to restore/recover the system at a particular state, at a particular point in time.
2. Electronic Media: Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
   1. Or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
3. Protected Health Information (PHI): Individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
   1. Past, present or future physical or mental health or condition of an individual.
   2. The provision of health care to an individual.
   3. Past, present, or future payment for the provision of health care to an individual.
   4. Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.
4. Electronic Protected Health Information (ePHI): Protected health information (PHI) under HIPAA that is transmitted by or stored by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
5. Hardware: Physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks, such as the mechanical, magnetic, electronic, and electrical components making up a computer system.
6. Off-Site: Any location separate from the building in which the backup was created. It must be physically separate from the creating site. The environment for off-site storage must meet appropriate security requirements as well as storage standards established by the manufacturer of the backup media.

**Policy:**

1. The Security Officer will be responsible for implementing this policy and will ensure that further responsibility is properly assigned for the proper management of data.
2. The [Insert Covered Entity or Business Associate name] Security Officer or designee is responsible for completing the backups and for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media and for performing periodic testing of restored media.
3. The Security Officer or designee shall maintain a record of movements of hardware and electronic media containing ePHI and any person responsible therefore.
4. Data Backup
   1. A backup, recovery and testing strategy should be determined based upon the [Insert Covered Entity or Business Associate name] Risk Analysis strategy.
   2. [Insert Covered Entity or Business Associate name] shall create a retrievable, exact copy of ePHI before movement of equipment.
      1. In the event a system does not allow for an electronic backup, [Insert Covered Entity or Business Associate name] will develop an alternative method to create a copy of the ePHI contained on that system, or complete an analysis delineating alternate solutions for compliance (such as a printed copy).
   3. In order to protect the confidentiality, integrity, and availability of ePHI, [Insert Covered Entity or Business Associate name] completes backups every (day, week, month, etc.).
   4. [Insert Covered Entity or Business Associate name] will perform a daily (at a minimum) backup of all systems that create, receive, maintain, or transmit ePHI. While a vendor may specify or recommend a full back up, an incremental back up, or may not specify, the Security Officer will determine the frequency with which backups are performed, dependent upon each system.
   5. Data backup systems may be manual or automated.
      1. Automated systems electronically capture backup locations, date/time, etc.
      2. If the process is manual, documentation of the backup should include:
         1. Site/location name
         2. Name of the system
         3. Type of data
         4. Date & time of backup
         5. Where backup stored (or to whom it was provided)
         6. Signature of individual that completed the back up
   6. The data backup plan requires that all media used for backing up ePHI is stored in a physically secure environment, such as a secure, off-site storage facility.
      1. If backup media remains on-site, it must be in a physically secure location, different from the location of the computer systems it backed up in order to protect the backups from loss or damage.
   7. If an off-site storage facility or backup service is used, a Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.
   8. Stored data must be accessible and retrievable at all times and all data backups should be tested and data restored to ensure accuracy.
   9. When reusable media are used as the backup media refer to the “Device, Media, and Paper Record Sanitization for Disposal or Reuse” policy.
   10. Data Backups should be tested and data restored, to assure accuracy. Documentation of backup testing, or restore logs, should be maintained and should capture the date and time the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed.
   11. Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences, should be addressed in the Disaster Recovery Plans.
5. Destruction
   1. [Insert Covered Entity or Business Associate name] will determine a record retention policy and data backup retention schedule. This schedule should include a timeline for ultimate destruction (tapes maintained and destroyed) of storage media.
6. Media Movement
   1. It is not possible or economically practical to control all media that enter and leave an organization. [Insert Covered Entity or Business Associate name] makes all reasonable and prudent efforts to control media entering and leaving the organization. Workforce members are trained to handle media with PHI in a manner which protects the confidentiality of the data contained on it. Media that contains PHI that is no longer useful or useable should be sanitized consistent with the “Device, Media, and Paper Record Sanitization for Disposal or Reuse” policy.
7. Documentation
   1. All documentation required by this policy will be maintained for a period of six years from the date of creation or the date when it was last in effect, whichever is later.

**Violations:**

1. Failure to back up a system in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment.
2. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.
3. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges.
4. Violation may also result in civil and criminal penalties to [Insert Covered Entity or Business Associate name] as determined by federal and state laws and regulations related to loss of data.
5. Violation may also result in liability to [Insert Covered Entity or Business Associate name] related to loss of data.