

# Data Management and Backup Policy

## **Policy:**

Kewaunee County establishes and implements procedures to create and maintain retrievable exact copies of electronic protected health information. The policy and procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all information systems used by Kewaunee County.

Kewaunee County creates a retrievable exact copy of electronic protected health information (ePHI) before movement of equipment.

Data back-up and the correct storage of backup media are an import part of the day to day operations of Kewaunee County's information security. To protect the confidentiality, integrity, and availability of ePHI, the organization completes backups daily. Established guidelines and defined standards for accountability of hardware and electronic media containing ePHI further provide the confidentiality and security of ePHI.

## **Responsible for Implementation:**

Security Officer

## **Applicable To:**

Any department or business associate that purchases, moves, maintains, and/or creates equipment or media capable of storing or transmitting ePHI.

## **Key Definitions:**

**Backup:** The process of making an electronic copy of data stored in a computer system. Examples of Back-ups Include:

- Full/Complete Backup - a backup/image of all (selected) data, programs, files on the system.
- Incremental Backup - a backup that only contains the files that have changed since the most recent backup (either full or incremental).
- Snap-shot back-up (image backup) – a process to restore/recover the system at a particular state, at a particular point in time

In the event a system does not allow for an electronic backup, Kewaunee County 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).

**Data Custodians** – persons responsible for keeping data and information organized and secure including rearranging data, renaming documents and other, similar activities but does not personally own or create the data.

Data Owners – persons who have the responsibility and authority to access, create and modify certain data as well as authorize or deny access by others to that data, and is responsible for its confidentiality, integrity and availability.

Electronic Media – means:

- 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;
- 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.

Electronic Protected Health Information (ePHI) - any individually identifiable health information protected (protected health information – PHI) by HIPAA that is transmitted by or stored by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Hardware - any 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, i.e., the mechanical, magnetic, electronic, and electrical components making up a computer system.

Off-Site: for the purpose of storage of back up media, off-site is defined as 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.

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:

- past, present or future physical or mental health or condition of an individual;
- the provision of health care to an individual;
- past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

Recovery Point Objective (RPO) - the age of files that must be recovered from backup storage for normal operations to resume.

Response Time Objective (RTO) - the maximum tolerable time limit within which data must be recovered; target time set for resumption of product, service or activity delivery after an incident.

### **Procedures:**

#### 1. Data Backup

- (a) A backup, recovery and testing strategy should be determined based upon Kewaunee County's Risk Analysis strategy
  - 1. The Information/HIPAA Security Officer has oversight responsibility and will ensure that further responsibility is properly assigned for the proper management of data.
  - 2. Kewaunee County's IT Director 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. Kewaunee County will perform a daily backup of all systems that create, receive, maintain, or transmit ePHI.
  - 4. Data backup systems are automated.
- (b) 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 or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
- (c) 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.
- (d) Stored data must be accessible and retrievable at all times.
- (e) All data backups should be tested and data restored to ensure accuracy.
- (f) When reusable media such as tapes are used as the backup media refer to the Device Sanitization and Disposal Policy.
- (g) Data Back-ups 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.
- (h) Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences, should be addressed in the Kewaunee County Disaster Recovery and Business Continuity Plans.

#### 2. Destruction

The Kewaunee County will determine a record retention policy and data backup retention schedule. This schedule should include a timeline for ultimate destruction of storage media.

#### 3. Media Movement

It is not possible or economically practical to control all media that enter and leave an organization. Kewaunee County makes all reasonable and prudent

efforts to control media entering and leaving the organization. Workforce members are trained to recognize that media containing ePHI is handled in a manner to protect 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 Sanitation and Disposal Policy.

4. Documentation

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.

5. Sanctions

- (a) 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.
- (b) Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.
- (c) 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.
- (d) Violation may also result in civil and criminal penalties to Kewaunee County as determined by federal and state laws and regulations related to loss of data.
- (e) Violation may also result in liability to Kewaunee County related to loss of data.