

**Polk County Wisconsin**  
**ADMINISTRATIVE SAFEGUARDS**  
**Contingency Plan**  
**Data Backup Plan Policy and Procedures**  
**45 CFR §164.308 (a)(7)(ii)(A)**  
**Required**

**Policy 602.K**

**Effective Date: October 12, 2004**

**Revised Date:**

## **Policy**

- A. Polk County Government will establish and implement policies and procedures to create and maintain retrievable exact copies of electronic protected health information (EPHI).
- B. The Information Technology Department will be responsible for implementation and oversight of procedures for creating and maintaining retrievable exact copies of EPHI.

## **Procedures**

- A. Polk County Government will develop and implement policies and procedures for data backup of all EPHI as required by the Security Rule.
- B. The Information Technology Department will be responsible for development, implementation and oversight of the Data Backup Plan so that a readily retrievable exact copy of EPHI is available.
- C. Factors to be considered in determining a data backup system may include the following:
  - 1. Capacity of the backup system.
  - 2. Type of storage media used (CD, disk, etc.).
  - 3. Potential for expanding the backup system.
  - 4. Simplicity of backup process. (A tedious, cumbersome system will impede workforce members in assisting in the backup process.)
  - 5. Dependability of backup system.
- D. The Information Technology Department will designate an individual to supervise the data backup process [Supervisor of Data Backup].

- E. The duties of the supervisor of the data backup process [or Security Officer] will include:
1. Identification of all input or data collection sites of EPHI.
  2. Identification of a data backup process, such as backup of every data set with exact copies, for each data collection site.
  3. Identification of a specific time frame when data backup processes are to be performed, such as requiring a daily data backup process to be performed at each data collection site at the end of every workday.
  4. Collection and secure storage of all backup data [on a daily basis].
  5. Maintenance of an inventory of all backups performed, collected and location in storage.
  6. Monitoring the data backup processes.
  7. Evaluation and testing of the security of the data backup processes.
  8. Training and monitoring of all personnel involved in the data backup processes.
- F. The supervisor of the data backup plan [or Security Officer] will identify all input or data collection sites of EPHI. See *Data Backup Plan Inventory of Sites Form*.
1. All input or data collection sites of EPHI will be identified and documented.
  2. All personnel provided access to EPHI at an identified data collection site will be identified and documented by job title, name and data collection site.
- Note:** A critical element of electronic information is the capacity to backup the electronic system. Threats to security of the electronic system may include hardware and/or software failures, power outages, theft, unauthorized access, human error and natural disasters such as fire, wind and rain.
- G. The Information Technology Department will identify a data backup process for each data collection site. The data backup processes may include the following or other processes as appropriate for the data collection site.
1. Backup of every set of data with exact copies [using disk or CD-Rom format].
- H. The Information Technology Department will train all workforce members involved with access or input at a data collection site on data backup processes.
1. Each workforce member will sign an attendance roster and an acknowledgement of data backup training.
  2. The documentation will be collected by the supervisor and maintained by the Information Technology Department.
- I. Data backup will be implemented [daily at the end of the regular work day or work shift] by the designated workforce member at the data collection site. Data

backup will be documented for every data backup process by the workforce member implementing the data backup process by completing the entry information on the *Data Backup Entry Form*, signing and dating the entry.

- J. *Data Backup Entry Forms* will be sent [on a daily basis] to the Information Technology Department. The Information Technology Department will be responsible for maintaining and retaining the *Data Backup Entry Forms*. The forms will be retained for a minimum of six years from the date of creation.

**Note:** Remember that the concept of backup is simply a process for copying files to another medium in case the primary medium fails. The most important aspect of backup is to do it regularly and consistently. Suggested methods for system backup may include:

- i. Tape Drive: A tape drive is a magnetic storage device (like a tape recorder) that may be separate from the central processing unit and reads data and writes it onto a tape. This is a sequential storage device, which means it limits access to the sequence in which it is stored.
- ii. Floppy Disk.
- iii. CD-ROM (Compact Disc – Read-Only Memory): A type of optical disk generally capable of storing larger amounts of data than a floppy disk. Use of the CD-ROM may allow for archiving digital information in a permanent storage manner.
- iv. Hard Drive: Backup techniques using hard drives include additional hard drives to allow copying from one hard drive to another and removable hard drives that allows removal and off-site storage of data.
- v. Internet Archiving: An Internet backup service may allow for backup to a remote location with little effort. Use of this option may require additional security such as encryption.