

Polk County Wisconsin
ADMINISTRATIVE SAFEGUARDS
Contingency Plan
Disaster Recovery Plan Policy and Procedures
45 CFR §164.308 (a)(7)(ii)(B)
Required

Policy 602.L

Effective Date: October 12, 2004 Revised Date:

Policy

- A. Polk County Government will establish (and implement as needed) procedures to restore any lost data caused by an emergency or other occurrence that damages systems that contain electronic protected health information (EPHI). The emergency or other occurrence may include fire, vandalism, power failure, system failure, natural disaster or a security incident.
- B. The Information Technology Department will be responsible for establishing (and implementing as needed) procedures to restore lost data.

Procedures

- A. The Information Technology Department will be responsible for establishing (and implementing as needed) a plan for the restoration of lost data as part of the plan for responding to an emergency or other occurrence that damages systems containing EPHI.
- B. The Information Technology Department will be responsible for coordinating the data recovery plan with the components of the *Data Backup Plan Policy and Procedures*. Effective data restoration will be contingent on effective recoverable data backup.
- C. The plan for restoration of lost data will include an assessment and listing of core processes/applications using EPHI. The list will be recorded on the *Disaster Plan Assessment Checklist*.
 - 1. The development of the plan will include a listing of potential occurrences that may cause system disruption to EPHI.
 - 2. The plan will include a statement of how the potential disaster event could affect the core process.

- D. The plan will include a reasonable solution for continuity of patient care information processes. The plan will include periodic review and testing. The solutions may include:
 - 1. An alternative uninterrupted power supply if the disaster event is a power outage.
 - 2. Location of servers and other critical hardware in a fire protection room or within a fire protected system.
 - 3. Containment of EPHI from wind or water damage.
- E. The plan will include immediate tasks for emergency containment. The tasks may include:
 - 1. Notification to the Information Technology Department of the disaster event.
 - 2. If computers have not automatically powered down, procedures to shut down systems.
 - 3. Disconnect power when necessary.
 - 4. Move all EPHI, equipment and/or systems away from disaster area.
- F. The disaster recovery plan will include a reasonable solution for restoration of data if interruption of EPHI or damage to EPHI occurs. The solution may include:
 - 1. Contacting the vendor.
 - 2. Contacting an electronic data recovery company.
 - 3. Reprinting or uploading documents from undamaged databases.
 - 4. Recovery from data backup systems.
- G. The Information Technology Department will document what EPHI and how EPHI was reconstructed.
- H. When data is lost or unable to be reconstructed, the Information Technology Department will document the date of loss, the information lost, the occurrence that led to information loss and attempted recovery methods.
- I. The Information Technology Department will create and maintain a record of the disaster event, a list of EPHI affected and successful and failed recovery efforts. The record will be retained for a minimum of six years from the date of creation.

Note: A contingency plan including restoration of data should be developed for each core process that contains EPHI and each potential disaster.