

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

Policy 602.N

Effective Date: October 12, 2004

Revision Date:

Policy

- A. Polk County Government will establish and implement policies and procedures for responding to 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, in coordination with the Privacy Officer, will be responsible for implementation and oversight of procedures for responding to an emergency or other occurrence that damages systems containing EPHI.

Procedures

- A. Polk County Government will develop and implement policies and procedures for responding to an emergency or other occurrence including the five implementation specifications required by the Security Rule.
- B. The Information Technology Department will be responsible for development; implementation and oversight of the contingency plan implementation specifications.
- C. Required Implementation Specifications.
 - 1. Data Backup Plan.

Information Technology Department will establish a data backup system so that a readily retrievable exact copy of EPHI is available. See *Data Backup Plan Policy and Procedures*.
 - 2. Disaster Recovery Plan.

The Information Technology Department will establish a plan to recover and/or restore any lost EPHI. See *Disaster Recovery Plan Policy and Procedures*.

3. Emergency Mode Operation Plan.

The Information Technology Department will establish an emergency mode operation plan to assure the continuation of critical data security processes during an emergency. See *Emergency Mode Operation Plan Policy and Procedures*.

D. Addressable Implementation Specification.

1. Testing and Revision Procedures

The Information Technology Department will test the contingency plan annually, or more frequently as necessary, and make any necessary revisions.

2. Applications and Data Criticality Analysis

The Information Technology Department will assess the relative criticality of specific applications and data as necessary to support other contingency plan components.