

**Polk County Government**  
**TECHNICAL SAFEGUARDS**  
**Access Control**  
**Emergency Access Policy and Procedures**  
**45 CFR §164.312 (a)(2)(ii)**

**Policy 602.Y**

**Effective Date: November 15, 2004**

**Revision Date:**

**I. Policy:**

- A. Polk County Government will establish, and implement as needed, procedures for obtaining necessary electronic protected health information (EPHI) during an emergency.
- B. This policy and procedures will regulate access to Polk County Government's EPHI during an emergency.
- C. The Information Technology Department will be responsible for development, implementation and monitoring of procedures for obtaining necessary EPHI during an emergency.

**II. Procedures**

- A. The Information Technology Department may utilize the emergency access procedures when any of the following occur:
  - 1. An incident that partially disables the central computing functions of Polk County Government.
  - 2. An incident that could potentially disable the central computing functions of Polk County Government.
  - 3. An incident that partially or completely disables the central computing functions of Polk County Government.
- B. The Information Technology Department, in coordination with governing department heads or Privacy Officer, will create a list that specifically identifies those who have been granted emergency access. This list will include the name of the individual granted access, job title, reason for emergency access, date access granted and name of individual granting access. The list will also include designation of backup individuals allowed emergency access if original listees are unavailable or unable to function. The list will include contact information for individuals granted emergency access.

1. All individuals authorized to have emergency access will be notified of the emergency access authorization.
  2. All individuals will be trained on procedures relating to emergency access.
- C. The Information Technology Department, in coordination with governing department heads or Privacy Officer, will delineate the procedures for emergency access. The procedures are to be utilized in an actual emergency, will bypass formal access procedures and are limited to emergency use. The procedures may include:
1. Creating a specific user account that provides full access to all EPHI
  2. Creating a second password rather than a separate account to provide full access.
  3. Other technical accessibility methods to allow immediate and full access.
- D. The emergency access will be tracked and documented based on capabilities of the system. The tracking documentation will be reviewed by the Information Technology Department or Privacy Officer, to determine that emergency access was appropriate. Any inappropriate emergency access will be treated as a security incident. *See Policy 602.M Security Incident Policy and Procedures.*
- E. Emergency access will be considered terminated as soon as it is no longer necessary.
- F. Inappropriate use of emergency access will be considered a reportable security incident and may subject an individual to immediate disciplinary action. *See 602.F Response and Reporting Policy and Procedures.*
- G. All activities related to emergency access will be documented by the Information Technology Department. The documentation will be retained and maintained for at least six years from the date of creation.