Polk County Government

TECHNICAL SAFEGUARDS

Access Control Policy and Procedures

45 CFR §164.312 (a)(1)

Policy 602.W
Effective Date: November 15, 2004 Revised Date:

I. Policy:

A. Polk County Government will implement technical policies and procedures for electronic information systems that maintain electronic protected health information (EPHI) to allow access only to those persons or software programs that have been granted access rights.

B. The Information Technology Department, in coordination with department heads and the Privacy Officer, will be responsible for development, implementation and monitoring of policies and procedures that allow access only to those persons or software programs that have been granted access rights.

C. Access controls will include:

1. Unique User Identification: The assignment of a unique name and/or number for identifying and tracking user activity.
2. Emergency Access Procedure: Establish and implement procedures for obtaining necessary EPHI during an emergency.
3. Automatic Log-off: Implementation of automatic log-off mechanisms that terminate access after a predetermined time of inactivity.
4. Encryption and Decryption: Implementation of a mechanism to encrypt and decrypt EPHI, to the extent reasonable, as a means of controlling access to EPHI.

D. Access controls are intended to regulate the following functions:

1. Provide authorized users access on information systems to perform functions necessary for their related workforce duties.
2. Regulate access according to the person or class of persons and functions they perform.

II. Procedures:

A. The Information Technology Department will be responsible for development, implementation and monitoring of policies and procedures for technical access controls.

B. Technical access controls will be implemented based on authorization of access determined by governing department heads over EPHI

C. The Information Technology Department will determine and implement appropriate technical access controls that are appropriate for Polk County Government.

D. Access controls will be established through system administrator accounts.

   1. The privileges provided to these accounts will permit the system administrator to add new user accounts, modify existing user accounts or terminate accounts.

   2. The system administrator account provides full access to the operating system, applications, system files privacy protected data files and audit trails.

E. The Information Technology Department will be responsible for documenting all activities related to technical access controls including all system administration activities. The documentation will be maintained and retained by the Privacy Officer for at least six years from the date of creation.