

Polk County Government
TECHNICAL SAFEGUARDS
Access Control
Unique User Identification Policy and Procedures
45 CFR §164.312 (a)(2)(i)

Policy 602.X

Effective Date: November 15, 2004

Revision Date:

I. Policy

- A. Polk County Government will implement policies and procedures to assign a unique name and/or number for identifying and tracking user identity.
- B. By the assignment of a unique name and/or number, it is the intent of Polk County Government to be able to uniquely identify and track a user or workforce member's access to all County-owned or operated networks, systems, and applications.
- C. The Information Technology Department will be responsible for developing and implementing policies and procedures for assigning a unique name and/or number for identifying and tracking user identity.

II. Procedures

- A. The Information Technology Department will complete a system assessment to determine capabilities of the system relating to assignment of unique user identification. The assessment may include:
 - 1. The Information Technology Department will first determine if the system provides a security access log-in mechanism.
 - a) If the system does not have log-in capabilities, a unique user identification cannot be assigned. Further development of the system may be required to develop log-in capabilities.
 - b) If the system has log-in capabilities, a unique user identification will be assigned.
 - 2. The Information Technology Department will determine if the system supports unique password access.
 - a) If the system does not support unique password access, further development of the system may be necessary to meet the Security Rule standard.
 - b) If the system supports unique password access, a unique password will be assigned.

- B. Allowing for system capabilities, the Information Technology Department, in coordination with governing department heads, Business Associates, or security application vendors, will assign every workforce member and any other person provided authorized access with a unique name or number that will provide authorized access to EPHI
 - 1. The assigned access code must be unique.
 - 2. The assigned access code cannot be a duplicate of another access code.
 - 3. There cannot be common user identification access codes.
 - 4. The unique identifier may be a password combining letters, numbers and/or symbols, a retinal scan, a thumbprint, a magnetic card or other access methods.
- C. When requesting access to County-owned or operated network, system or applications that accesses, transmits, receives or stores EPHI, a user or workforce member will be required to supply their assigned unique user identification to gain access to the above mentioned County-owned or operated networks, systems or applications.
- D. The workforce members or other authorized persons who are assigned unique access codes will be required to follow practices that maintain unique tracking capabilities and uniqueness of the code.
 - 1. Users with unique access codes are not allowed to share their unique access code with others.
 - 2. No-one other than the assigned user is allowed to use the unique access code.
 - 3. Users are not allowed to use, document or display their user identification in an unsecured manner.
- E. The assigning of the unique access code by the Information Technology Department, or other recognized authority, will be implemented in a manner that ensures identification and tracking of users of the information system. The assignment needs to exemplify that the system can control access to the data by denying access as well as allowing access.
 - 1. The system must exemplify that the unique password controls access.
 - 2. The system must exemplify that the unique password can deny access.
- F. The unique user identification will utilize a password assignment that incorporates current best practices in computer technology to ensure uniqueness and security of the unique identifier, including number of characters and potential for expansion.
- G. It is the responsibility of the user or workforce member to maintain their unique user identification in a protected manner and to ensure that it is only used for authorized access to County-owned or operated networks, systems or

applications. Compromise to the security of the unique user identification by a user or workforce member must be immediately reported to the Information Technology Department. *See Policy 602.F Response and Reporting Policy and Procedures.*

- H. A lost password must be reported immediately to the governing department head, or to the Information Technology Department and authorized access terminated.
- I. Failure to comply with these policy and procedures may result in immediate disciplinary action. *See Policy 716 Employee Discipline.*
- J. The Information Technology Department is responsible for reviewing and evaluating this policy and procedure on a periodic basis to ensure that they maintain technical compliance.
- K. The Information Technology Department, in coordination with governing department heads and Privacy Officer, will be responsible for documenting all activities that relate to assignment and use of unique user identification.
- L. The documentation will be maintained and retained by the Privacy Officer for a minimum of six years from the date of creation.