

Polk County Government
TECHNICAL SAFEGUARDS
Person or Identity Authentication Policy and Procedures
45 CFR §164.312 (d)

Policy 603.B

Effective Date: November 15, 2004 Revision Date:

I. Policy

- A. Polk County Government will implement procedures to verify that a person or entity seeking access to electronic protected health information (EPHI) is who he/she claims to be.
- B. The Information Technology Department, in coordination with governing department heads, Privacy Officer, Business Associates, or authorized security application vendors, will be responsible for development, implementation and monitoring of verification procedures.

II. Procedures

- A. The Information Technology Department will implement procedures to verify the identity of authorized users. Authentication procedures may include the following:
 - 1. All workforce members with authorized access to the network, system or application that contains EPHI must satisfy a user authentication mechanism. The authentication mechanism may include any of the following:
 - a) Use of a unique user identification and password.
 - b) Use of biometric input (fingerprint, retina scan).
 - c) Use of a user identification smart card (smart card, token, key swipe).
- B. The Information Technology Department, in coordination with governing department head, or Privacy Officer, will implement and enforce the following workforce controls to ensure the verification of the identity of authorized users.
 - 1. Workforce members with authorized access to any network, system or application are not allowed to misrepresent themselves by using another person's user identification and password, smart card, or other access control mechanism.

2. Workforce members are not allowed to permit other persons or entities to use their unique user identification and password, smart card, or other access control mechanism.
 3. A reasonable effort by all workforce members will be made to verify authenticity of the receiving person or entity prior to transmitting EPHI.
- C. Non-compliance with this policy may result in immediate employee disciplinary action. See *Policy 602.M Security Incident Policy and Procedures* and *Policy 601.P Confidentiality Policy*.
 - D. The Information Technology Department, to the extent reasonable, will monitor procedures to verify identity of authorized users.
 - E. The Information Technology Department, and Privacy Officer will document all activity related to verification of authenticity.
 - F. The Privacy Officer will maintain all documentation related to verification of authenticity for a minimum of six years from the date of creation.