

**Polk County Government**  
**TECHNICAL SAFEGUARDS**  
**Technical Safeguards Policy and Procedures**  
**45 CFR §164.312**

**Policy 602.V**

**Effective Date: November 15, 2004      Revised Date:**

**I. Policy**

- A. Polk County Government will develop and maintain technical safeguards to protect the integrity, confidentiality and availability of electronic protected health information (EPHI).
- B. The Information Technology Department will be responsible for oversight of the implementation and monitoring of technical safeguards required by the Security Rule.
- C. The technical safeguards developed and maintained will include:
  - 1. Access Control: Policies and procedures that technically allow access to EPHI only to authorized users.
  - 2. Audit Controls: Policy and procedures that establish hardware and/or software mechanisms to record and examine certain information system activity.
  - 3. Integrity: Policy and procedures to protect EPHI from being improperly altered or destroyed.
  - 4. Person or Identity Authentication: Policy and procedures to verify that a person or entity seeking access to EPHI is who they claim to be.
  - 5. Transmission Security: Policies and procedures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

**II. Procedures**

- A. The Information Technology Department will develop, implement and monitor the technical safeguards required by the Security Rule.
- B. The Information Technology Department will review and evaluate technical safeguards on an annual basis, or as needed, to ensure technical viability and effectiveness.
- C. The Information Technology Department will document, maintain and retain copies of all relevant technical safeguard activities.
- D. The documentation will be retained by the Privacy Officer for at least six years from the date of creation.