

Polk County Government
TECHNICAL SAFEGUARDS
Integrity Policy and Procedures
45 CFR §164.312 (C)(1)

Policy 603.A

Effective Date: November 15, 2004 Revision Date:

I. Policy

- A. Polk County Government will implement policies and procedures to protect electronic protected health information (EPHI) from improper alteration or destruction.
- B. The Information Technology Department will be responsible for implementation of policies and procedures to protect EPHI from improper alteration or destruction.
- C. The policies and procedures will include a mechanism to authenticate EPHI to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.
- D. Definition of Integrity: The property that data or information has not been altered or destroyed in an unauthorized manner.

Compromising data integrity may include:

- Human intervention.
- Hacking or unauthorized intrusion.
- Data input errors (human).
- Mechanical errors causing disruption to data retrieval.
- Transmission or receiving errors.
- Data interface issues.
- Malicious software, viruses.
- “Bugs” (programming problems).
- Magnetic exposure.

II. Procedures

- A. The Information Technology Department, in coordination with governing department heads, Privacy Officer, Business Associates, or authorized security application vendor, will implement all reasonable methods to ensure data integrity.
- B. Reasonable methods to be implemented to ensure data integrity may include:
 - 1. Review processes to ensure data entry accuracy:
 - a) By another workforce member, and/or
 - b) An application or program that edits for errors.
 - 2. Intrusion detection systems.
 - 3. Audit trails to prevent unauthorized access or use.
 - 4. Backup systems to prevent data loss. See *Policy 602.KData Backup Plan Policy and Procedures*.
 - 5. Implementation of integrity controls that detect or prevent transmission errors.
 - 6. Interface programs that result in data being synchronized, reconciled and shared.
 - 7. Software products that indicate corrected or improved versions.
 - 8. Antivirus software or other programs designed to identify malicious software.
 - 9. Prevent exposure of electronic media to excessive heat or magnetic field.
- C. The Information Technology Department and Privacy Officer will document all data integrity implementation activities. The documentation will be maintained and retained for a period of at least six years from the date of creation.