

Polk County Government
TECHNICAL SAFEGUARDS
Audit Controls Policy and Procedures
45 CFR §164.312 (b)

Policy 602.Z

Effective Date: November 15, 2004 Revision Date:

I. Policy

- A. Polk County Government will implement hardware, software and/or procedural mechanisms, to the extent reasonable, that record and examine activity in County owned information systems that contain or use electronic protected health information (EPHI). The mechanisms will provide evidence of identified system activities as well as an audit trail of activities performed.
- B. The Information Technology Department will be responsible for implementation of mechanisms that record and examine activity in the information systems.

II. Procedures

- A. The Information Technology Department will evaluate current hardware and software to determine whether they contain the capability to record and examine activity in the information system. Systems that contain EPHI may include County owned workstations, laptops, servers, personal data assistants (PDAs), other computing systems as well as electronic media.
 - 1. Can the hardware/software audit access?
 - 2. Can the hardware/software track activity in the system?
 - 3. Can the hardware/software track who is logging in and/or off, who is changing files and/or what are they changing?
- B. Based on the findings of the above evaluation, the Information Technology Department will take appropriate action.
 - 1. If the current hardware and software are capable of recording and examining activity in the information system, the Information Technology Department will continue to monitor and update the systems as appropriate, and reasonable.
 - 2. If the current hardware and software do not have recording and examining capabilities, the Information Technology Department, to the extent reasonable, will need to update the hardware and software to accomplish these activities.

- C. When possible, audit trails will be stored on a separate computer system to maintain the confidentiality of the audit trail. The audit trails will be accessible to the Information Technology Department.
- D. The Information Technology Department will document whether tracking is at the application level, computer level or computer network level.
- E. The Information Technology Department will notify workforce members that their activities may be monitored by an audit trail.
- F. The audit trail should provide the Information Technology Department with a chronological trail of computer events that gives information about an operating system, an application or user access. The audit trail will be used to monitor computer activity to assist in determining:
 - 1. Whether a security incident has occurred.
 - 2. Whether there is an indication of unauthorized access.
 - 3. Whether there is unusual workforce member access.
 - 4. Whether there is unusual activity that requires further investigation.
- G. The Information Technology Department will review the records of system activities. See *Policy 602.G Information System Activity Review Policy and Procedures*.
- H. The Information Technology Department will document the mechanisms that record and examine activity in the information systems. The documentation will be maintained by the Information Technology Department and the Privacy Officer for a minimum of six years from the date of creation.