Polk County Government

ADMINISTRATION SAFEGUARDS

Security Management Process Policy and Procedures

45 CFR 164.308 (a)(1)(i)

Policy 603.D
Effective Date: March 15, 2005 **Revision Date:**

I. Policy

A. Polk County Government will implement policies and procedures to prevent, detect, contain and correct security violations.

B. The security management process will include:

1. A risk analysis assessing potential risks to the confidentiality, integrity and accessibility of Polk County Government's electronic protected health information (EPHI).
2. Security measures to reduce risks.
3. A policy implementing appropriate sanctions against workforce members who fail to comply with Polk County Government's security policies and procedures.
4. Procedures to regularly review records of information system activity.

C. The Information Technology Department will be responsible for development, implementation and monitoring of the security management policies and procedures of Polk County Government .

II. Procedures

A. The Information Technology Department will be responsible for development, implementation and monitoring of the security management process of Polk County Government.

B. The security management process will include the following components:

1. A risk analysis that includes an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by Polk County Government.
2. A risk management process that implements security measures sufficient to reduce identified risks and vulnerabilities to a reasonable and appropriate level.

3. A sanction policy and procedures designed to implement appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Polk County Government.
4. Implementation of an information system activity review process that provides regular records reviewing all information system activity, including audit logs, access tracking reports and security incident notifications.