

**Polk County Wisconsin**  
**ADMINISTRATIVE SAFEGUARDS**  
**Security Management Process**  
**Risk Analysis Policy and Procedure**  
**§164.308 (a)(1)(ii)(A)**  
**Required**

**Policy 602.E**

**Effective Date: August 17, 2004**

**Revision Date:**

**Policy**

- A. Polk County Government will conduct a risk analysis to assess Polk County Government ability to prevent, detect, contain and correct security violations relating to electronic protected health information (EPHI).
- B. The risk analysis performed by Polk County Government will include an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by Polk County Government.
- C. The Information Technology Department of Polk County Government will be responsible for developing, performing and documenting Polk County Government risk analysis.

**Procedures**

- A. The Information Technology Department will develop and conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by Polk County Government.
- B. The Information Technology Department will utilize a risk analysis process to identify potential security risks and vulnerabilities and determine how best to apply the safeguards required by the Security Rule. See *Risk Management Policy and Procedures*.
- C. The Information Technology Department will conduct a risk analysis that compares the requirements of the Security Rule with currently implemented security processes. Completion of the risk analysis will be done on the *Risk Analysis Form*. The following will be documented in relation to the requirements of the Security Rule to ascertain a baseline compliance status: “Yes” to indicate in compliance, “In Progress” to indicate the requirement is being worked on, “No” to indicate currently not in compliance, “Not Applicable” or “Unsure”. The

resulting data will be used to formulate a plan for compliance as part of the risk management process.

- D. The Information Technology Department will compile a comprehensive inventory documenting the major components/structure of Polk County Government electronic information system. See *Risk Analysis Repository Inventory Form*. The process documenting the components of Polk County Government electronic information system will include:
1. Identification and logging of all repositories of EPHI on a common inventory document. Repositories of EPHI to be identified and logged may be in the form of a database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more users.
  2. The repository inventory will be documented on the *Risk Analysis Repository Inventory Form*.
  3. An ongoing inventory of repositories will be performed annually or as necessary to ensure that the EPHI repository inventory is current and comprehensive.
- E. The Information Technology Department will fill out a *Security Management Form* for each repository identified on the *Risk Analysis Repository Inventory Form*. For each repository, the following data will be collected on the *Security Management Form*.
1. The title of the repository.
  2. The relevant Security Rule requirement(s) or applicable security safeguard(s).
  3. The vulnerability identifying a weakness or gap relating to the repository. The Information Technology Department will identify and document vulnerabilities to Polk County Government electronic information system.
    - a) Each identified repository will be analyzed for potential vulnerability to the confidentiality, integrity and availability of its EPHI.
    - b) The Information Technology Department will utilize the Security Rule standards and implementation specifications to perform a baseline analysis of vulnerabilities.
  4. Any potential threat presenting as an indication or warning of trouble. The Information Technology Department will identify and document threats to each component of Polk County Government electronic information system.
    - a) Human threats: Intentional, unintentional.
    - b) Natural threats: Earthquakes, wind, water.
    - c) Environmental threats: Fire, toxic materials, power outage, water leakage, broken pipes, heating, and ventilation.

5. The probability that the threat is likely to occur. The Information Technology Department will identify and document the potential of a threat event to each component of Polk County Government electronic information system. A threat event would be the resulting consequences of a threat.
    - a) Unauthorized access to EPHI (confidentiality).
    - b) Loss, defacement or tampering of EPHI (Integrity).
    - c) Interruption of access to EPHI (Availability).
    - d) The impact of the threat, were it to occur.
  6. The overall potential that a threat would occur that would result in high impact. The Information Technology Department will determine and document the potential for a threat attacking a vulnerability (a security breach) and the potential impact to the information system (determine a level of risk).
    - a) Each identified repository will be assigned a level of risk based on the amount of EPHI in the repository and the number of users accessing the EPHI. The level of risk may also be assigned based on the degree of sensitivity of the EPHI.
    - b) High risk: Large number of records accessed by a large number of users. May also include EPHI that may be classified as highly sensitive regardless of the number of records and/or users.
    - c) Medium Risk: Large number of records and small number of users or small number of records and large number of users.
    - d) Low Risk: Small number of records with small number of users.
  7. The final column, documenting a work plan to address the vulnerability and prevent a threat occurrence will be completed in the risk management process.
- F. The Information Technology Department will document the risk management processes and maintain the documentation for a minimum of six years from the date of creation.
- G. The Information Technology Department will [periodically/annually] review and update the risk analysis to make any necessary adjustments to adapt to technology changes and to maintain compliance with the Security Rule.