

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

Policy 602.D

Effective Date: August 17, 2004 Revision Date:

Policy

- A. Polk County Government will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the General Rules of the Security Standards of the Security Rule. The General Rules require:
1. That Polk County Government will ensure the confidentiality, integrity and availability of all Polk County Government electronic protected health information (EPHI).
 2. That Polk County Government will protect against any reasonably anticipated threats or hazards to the security of Polk County Government EPHI.
 3. That Polk County Government will protect against any unreasonably anticipated uses or disclosures of Polk County Government EPHI.
 4. That Polk County Government will ensure compliance with the Security Rule.
 5. That Polk County Government may use any security measures that allow Polk County Government to reasonably and appropriately implement the standards and implementation requirements of the Security Rule and the measures may be determined by the size, complexity and capabilities of Polk County Government.
- B. The Information Technology Department will be responsible for implementing security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

Procedures

- A. The Information Technology Department will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

- B. The Information Technology Department will utilize the *Risk Analysis Form*, compiled to indicate compliance with the requirements of the Security Rule, to focus security management efforts and develop a strategy to meet the Security Rule requirements.
1. Requirements documented with “Yes”, indicating compliance, will be supplemented with additional documentation that specifies very clearly the processes that are in place that meet the Security Rule requirements.
 2. Requirements documented with “In Progress”, indicating some measures are in place relating to the Security requirement, will be supplemented with additional documentation that specifies very clearly the processes in place and the additional components necessary to meet the Security Rule requirements.
 3. Requirements documented with “No”, indicating no compliance at this time, will be supplemented with additional documentation that specifies very clearly the processes that will be developed and implemented and a timeframe for completion.
 4. Requirements documented with “NA”, indicate this specific requirement of the Security Rule is not applicable to Polk County Government.
 5. Requirements documented with “Unsure”, indicate that further information and resourcing needs to occur before a compliance assessment can take place. These requirements will be marked for additional work and a timeframe for meeting compliance once further education has occurred will be developed and documented.
 6. Utilizing this process, the Information Technology Department will address each Security Rule requirement, the current compliance status of Polk County Government and develop an appropriate security management process to address the identified gaps in Polk County Government current security safeguards.
 7. The resulting document will be used to formulate a security management process that will be used to develop, implement and monitor compliant security safeguards.
- C. The Information Technology Department will review the *Risk Analysis Repository Inventory Form* and evaluate the current compliance status of all electronic information repositories. The data collected on the *Risk Analysis Repository Inventory Form* will be utilized to determine where to focus security risk management efforts.
1. The final column of the *Risk Management Form* will be completed as part of the security management process. For each identified repository, a work plan will be developed to address the vulnerability and prevent a threat occurrence.
 2. The repositories of EPHI may also be identified and classified as low, medium or high risk as part of the repository data collection process.

3. Repositories identified as high and medium risk will be subject to the full extent of the security policies.
 4. Sufficient security measures will be implemented for each repository.
- D. The security management process will include utilization of the risk analysis performed in the *Risk Analysis Policy and Procedures* and documented on the *Risk Management Form*.
1. The *Risk Management Form* identified the Security Rule requirement, Polk County Government vulnerability in relation to that requirement, the potential threat to Polk County Government relating to that requirement, the probability of occurrence, the magnitude of harm that could result and an overall summary of risk.
 2. The security management process will address each Security Rule requirement as it relates to Polk County Government, its vulnerabilities and potential threats and develop an appropriate security management process to address the identified risks. See *Risk Management Form*.
- E. The Information Technology Department will be responsible for utilizing the *Risk Analysis Form*, the *Risk Analysis Repository Inventory Form*, the *Risk Management Form* and any other risk assessment tools and/or processes to develop and implement comprehensive and effective security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.
- F. The Information Technology Department will document the risk management procedures and maintain the documentation for a minimum of six years from the date of creation.