

**Polk County Wisconsin**  
**ADMINISTRATIVE SAFEGUARDS**  
**Evaluation Policy and Procedures**  
**45 CFR §164.308 (a)(8)**  
**Required**

**Policy 602.J**

**Effective Date: October 12, 2004      Revised Date:**

## **Policy**

- A. Polk County Government will perform a periodic technical and non-technical evaluation, based upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information (EPHI), that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule.
- B. The Information Technology Department, in coordination with the Privacy Officer and HIPAA Committee members, will be responsible for development and implementation of a periodic technical and non-technical evaluation that assesses the extent to which Polk County Government security policies and procedures meet the requirements of the Security Rule.

## **Procedures**

- A. The Information Technology Department will be responsible for the periodic evaluation of HIPAA Security compliance procedures to ensure that they maintain their technical and non-technical viability and continue to comply with the Security Rule.
  - 1. The security policies and procedures will be reviewed annually and may be structured for review on a monthly basis.
  - 2. The review, all, or in part, shall be performed by the Information Technology Department, Privacy Officer, or a HIPAA Committee member (Documentation will be the responsibility of the party, or parties, performing the review).

- B. The evaluation will include:
  - 1. An assessment of whether there are policies and procedures developed and implemented in compliance with the Security Rule requirements. (Are the required policies and procedures developed and implemented?)
  - 2. An assessment of whether the policies and procedures are functioning in a manner to protect confidentiality, integrity and availability of EPHI. (Are they functioning as anticipated?)
  - 3. A periodic review of the effectiveness of security policies and procedures. (Are they truly effective in providing security safeguards?)
- C. Subsequent evaluations may be based on:
  - 1. An analysis of security incidents.
  - 2. Changes in practice.
  - 3. New technology.
- D. A policy evaluation may need to be performed other than at the normally scheduled periodic time based on one of the following occurrences:
  - 1. Changes in the Security or Privacy Rules.
  - 2. New federal, state or local regulations affecting HIPAA.
  - 3. Changes in environmental and/or business processes that may affect security safeguards.
  - 4. A serious security incident.
  - 5. A significant change in operations.
  - 6. Significant security threats in the environment.
- E. The Information Technology Department, in coordination with the Privacy Officer or HIPAA Committee members, will implement any necessary changes.
- F. The Information Technology Department, in coordination with the Privacy Officer will be responsible for documentation, collection of documentation, maintenance and retention of any information relating to periodic evaluations of security policies and procedures including periodic evaluation reports, analyses, recommendations and/or changes made. See *Evaluation Security Grid Form*.
- G. The documentation shall be maintained by the Privacy Officer for at least six years from the date of creation.