

Polk County Wisconsin
ADMINISTRATIVE SAFEGUARDS
Security Incident Procedures
Response and Reporting Policy and Procedures
45 CFR §164.308 (a)(6)
Required

Policy 602.F

Effective Date: October 12, 2004 Revision Date:

Policy

- A. Polk County Government will implement policies and procedures in compliance with the Security Rule to identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to Polk County Government; and document security incidents and their outcomes.
- B. A security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. [45 CFR 164.304]
- C. The Information Technology Department in coordination with the Privacy Officer will be responsible for development, implementation and monitoring of policies and procedures related to response and reporting of security incidents.
- D. A security incident means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. [45 CFR 164.304]

A security incident may include any of the following:

- 1. Sharing of unique passwords.
- 2. Unauthorized use of passwords.
- 3. Tampering with the integrity of data.
- 4. Unauthorized access (internal or external).
- 5. Attempts at unauthorized access (internal or external).
- 6. Virus infiltration.
- 7. Incidents that could undermine the security or reliability of the information system.

Procedures

- A. The Information Technology Department in coordination with the Privacy Officer will develop, implement and monitor policies and procedures to identify and respond to suspected or known security incidents.
- B. The Information Technology Department will identify to the extent possible, potential security incidents that may occur to electronic protected health information (EPHI) maintained by Polk County Government.
- C. Training.
 - 1. The Information Technology Department in coordination with the Privacy Officer shall ensure that all workforce members be trained on identification, response, reporting and mitigation relating to security incidents.
- D. Identification and Reporting.
 - 1. All workforce members will identify and report any actual, attempted or threatened breach of security of EPHI and the outcome to the Information Technology Department.
 - 2. Reporting of security incidents by workforce members or other persons will be made to their immediate supervisor and the Information Technology Director as soon as possible after the incident has been identified. Immediacy of reporting is critical to resolution and the importance of the timeliness of reporting will be conveyed in workforce training sessions. Under no circumstances should a known incident be unreported for more than 24 business hours.
 - 3. Reporting a security incident will be considered a contribution toward improvement of patient services and there will be no retaliation for reporting security incidents.
 - 4. Reporting of security incidents may be made in whatever appropriate manner that clearly communicates the security incident to the Information Technology Department. Reporting may be made by written notice, e-mail, phone, oral presentation or other appropriate method.
 - 5. The Information Technology Department will attempt to preserve all evidence of the security incident.
 - 6. The Information Technology Department will document all security incidents and their outcome either identified by the Information Technology Department or reported by the workforce or others to the Information Technology Department in the *Security Incident Log*.

7. The Information Technology Department will also document any other security issues and outcomes in the *Security Incident Log*.

E. Investigation.

1. The Security Officer and/or Privacy Officer will investigate any identified security violation. See *Investigation of Security Incident Policy and Procedures*.
2. The Security Officer and/or Privacy Officer will make a reasonable attempt to identify the cause and effect, if any, of the security incident. All recoverable documentation of cause and effect will be preserved and maintained to the extent reasonably possible.
3. The Security Officer and/or Privacy Officer will document the investigation process relating to the security incident on the *Investigation of Security Incident Form*.

F. Response.

1. The Information Technology Department will address all security incidents on a case-by-case basis.
2. The Information Technology Department will have the responsibility and authority to take or direct appropriate action to address the security issue.
3. All security incidents will be corrected in a manner that will prevent any ongoing or future incidents. Corrective action may include the following:
 - a) Technology changes.
 - b) Procedure review or revision.
 - c) Workforce (re-) training.
 - d) Sanctions as necessary.
4. Corrective actions will be designed to ensure that the specific security issue addressed and similar problems do not recur in the future.
5. Employees knowledgeable of and/or engaged in intentional security violations will be subject to corrective and/or disciplinary action, up to and including termination in appropriate cases, in accordance with *Policy 601.P Confidentiality, Security and Access to PHI and Policy 716 Employee Discipline*.
6. Confidentiality of EPHI will be maintained while investigating, reporting and responding to security violations.
7. The Information Technology Department will document all responses to identified and/or known security incidents.

G. Prevention.

1. The Information Technology Department will implement all necessary precautions to ensure that the documented security incident does not recur.

H. Mitigation.

1. The Information Technology Department will mitigate, to the extent practicable, harmful effects of security incidents that are known to the Information Technology Department.
- 2.
2. Mitigation may include:
 - a) Prevention of future security incidents.
 - b) Notification of affected individuals.
 - c) Provision of assurances to affected individuals.
 - d) Continued monitoring of the security incident to prevent future occurrences.

I. Documentation.

1. The Information Technology Department will document all security incident processes, including security incidents, outcomes, corrective action and mitigation taken in the *Security Incident Log*. The *Log* will contain documentation of the identified security issue and the individual(s) or department(s) affected.
2. The documentation will be maintained by the Privacy Officer for a minimum of six years from the date the documentation was created.
3. All documentation relating to security incidents will be maintained in a confidential manner that respects and protects the privacy of patient health care information.