

Policy and Procedure Number:
Effective:

Security Incidents Reporting and Response

Purpose

The Jackson County Health Department is committed to maintaining formal practices to manage the election and execution of security measures to protect patient and other data and to manage the conduct of personnel in relation to patient and other data. As such, Jackson County Health Department will continually assess potential risks and vulnerabilities to individual health data in its possession, and develop, implement, and maintain appropriate security measures.

Policy

1. The policies and procedures herein apply to all electronically maintained or transmitted health information pertaining to an individual.
2. Employees, contractors, and others will immediately report any and all suspected and actual breaches of information security to the Information Security Officer.
3. The procedures herein will be referenced to and coordinated with the Contingency Plan in this manual.
4. The Information Security Officer for the Jackson County Health Department is responsible for determining the appropriate level of response to a security incident, in accordance with the Jackson County Health Department documented policies and procedures.
5. All incident reporting and response activities will be conducted strictly on a need-to-know basis.
6. All employees will be trained regarding appropriate reporting of security breaches.
7. Security incident policies and procedures will be updated as needed.

Procedures

1. Employees suspecting a malicious code infection will immediately notify the Security Officer by phone or walk-in. Email will not be used. Employees may be asked to supply the following information, which will be documented by the Security Officer in his/her formal report:
 - a. Name and phone number of person reporting the incident
 - b. Date and time the incident was discovered
 - c. Observed behaviors that led to the incident being suspected
 - d. Any unusual circumstances surrounding the event.
2. The Security Officer will respond to the reported security incident in the following manner:
 - a. Disconnect the affected component(s) from the network, without removing power from the component.
 - b. Determine if the reported incident is actually a security breach.
 - c. Record all findings, being sure to carefully sign and date all documents.
 - d. Ensure that all evidence (disks, CDS, etc.) is sealed in secure containers and that

- access to these items is controlled.
 - e. Notify law enforcement and the Office of Management Information Systems (OMIS) if necessary.
 - f. Back up the compromised machine to unused media, controlling such evidence as noted above. Make additional, separate backups for investigation and/or restoration purposes.
 - g. Assess the risk on continuing operations, consulting with the Office of Management Information Systems (OMIS).
 - h. Change or revoke passwords used on the affected systems/network.
 - i. Make changes necessary to address vulnerabilities exploited with respect to the incident.
3. The policies and procedures established herein, including all derivative documents regarding security breaches, reports, and responses will be documented using the Incident Report and will be maintained by the Information Security Officer.