

Security Incident Response Policy

Policy:

An information security incident response process is implemented to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

This policy has been developed to address the HIPAA Security Rule standard for security incident procedures and as supplemented by HITECH provisions of American Recovery and Reinvestment Act (“ARRA”).

It is the policy of Kewaunee County to safeguard the confidentiality, integrity, and availability of operational and patient protected health information through an established information security incident response process. The information security incident response process addresses:

- Continuous monitoring of threats through intrusion detection systems (IDS) and other monitoring applications;
- Establishment of an information security incident response team;
- Establishment of procedures to respond to media inquiries;
- Establishment of clear procedures for identifying, responding, assessing, analyzing, and follow-up of information security incidents;
- Workforce training, education, and awareness on information security incidents and required responses; and
- Facilitation of clear communication of information security incidents with internal, as well as external, stakeholders

Responsible for Implementation:

Individuals needed and responsible to respond to a security incident make up a Security Incident Response Team (SIRT). Membership on the SIRT may vary depending on the nature of the incident and may vary during the course of the investigation and remediation of the incident.

Applicable To:

All workforce members/staff, departments, contractors and business partners of Kewaunee County must adhere to the Security Incident Response Policy.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Purpose:

The purpose of this policy is to establish guidelines for the identification, response, reporting, assessment, analysis, and follow-up to all suspected information security

incidents. The information security response process helps to ensure the security, confidentiality, integrity and availability of electronic information and the automated systems that contain it and the networks over which it travels.

Scope:

This policy applies to the following security incidents:

- Technical security incidents
- Non-technical security incidents

Key Definitions:

Electronic Protected Health Information (ePHI): any individually identifiable health information protected (protected health information – PHI) by HIPAA that is transmitted by or stored by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Event: an occurrence that does not constitute a serious adverse effect on the organization or its operations, though it may be less than optimal.

- An adverse event is any observable computer security-related occurrence in a system or network with a negative consequence. Events require an analysis to determine their impact on the system or network to determine if the definition of an “event” is met. All events do not require a formal Security Incident Response.
- Examples of events include, but are not limited to:
 - A hard drive malfunction that requires replacement
 - Systems become unavailable due to power outage that is non-hostile in nature
 - Accidental lockout of an account due to incorrectly entering a password multiple times
 - Network or system instability

Indication: A sign that an incident may have occurred or may be occurring at the present time. Examples of indications include:

- The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS “hits” are also false positives and are neither an event nor an incident.
- The antivirus software alerts when it detects that a host is infected with a worm.
- The Web server crashes.
- Users complain of slow access to hosts on the Internet.
- The system administrator sees a filename with unusual characteristics.
- The user calls the help desk to report a threatening e-mail message (and it is determined by Information Services that it is a legitimate risk issue).
- Other events that are not normal to the operation of an individual system

Precursor: A sign that an incident may occur in the future. Examples of precursors include:

- Suspicious network and host-based IDS events/attacks.

- Alerts as a result of detecting malicious code at the network and host levels.
- Alerts from file integrity checking software.
- Alerts from third party monitoring services.
- Audit log alerts.

Information/Computer Security Incident: a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

- An incident is the culmination of one or more events with adverse effects.
- An “imminent threat of violation” refers to a situation in which the organization has a factual basis for believing a specific incident is about to occur.

Security incidents include, but are not limited to:

- A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious
- Unauthorized disclosure
- Unauthorized change or destruction of ePHI
- Physical threat to staff members or external entities at the site
- Physical intrusion/security incident/active shooter
- Biological threat to staff members or external entities at the site (e.g., bioterrorism attacks, such as those conducted through use of toxins such as anthrax)
- Disaster or enacted threat to business continuity
- Examples of information security incidents may include, but are not limited to, the following:
 - **Denial of Service:** An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
 - **Malicious Code:** An Advanced Persistent Threat (APT) such as a worm, virus, Trojan horse, ransom ware or other code-based malicious entity that infects a host.
 - **Unauthorized Access/System Hijacking:** A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations.
 - **Inappropriate Usage:** A person violates acceptable computing use policies.
 - **Unplanned Downtime:** The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime (e.g., system failure, utility failure, disaster situation, etc.).
 - **Multiple Component:** A single incident that encompasses two or more incidents (e.g., a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts).
- Other examples of observable information security incidents may include, but are not limited to:
 - Use of another person’s individual password and/or account to login to a system.
 - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment).
 - Leaving workstations unattended while actively signed on.

- Installation of unauthorized software.
- Falsification of information.
- Theft of equipment or software.
- Destruction of tampering with equipment or software.
- Posting of PHI on the Internet from a web portal.
- Discarding of PC hard drives, CDs or other devices including PHI without following approved destruction/disposal guidelines.
- Terminated workforce member accessing applications, systems, or network.

Procedures

The security incident response process that follows reflects the process recommended by NIST and SANS. Process flows are a direct representation of the SANS process. The Containment, Eradication, and Recovery Phases are highly technical and it is important to have them completed by a highly qualified technical security resource with oversight by the SIRT team.

1. Preparation and Identification/Detection Phase (Phase I):

- (a) Immediately upon observation, workforce members must report suspected and known precursors, events, indications, and security incidents to a direct supervisor, Security Official or County Administrator.
- (b) The individual who receives the report notifies the Security Official.
- (c) The Security Official assesses the validity of the information and determines if the issue is a precursor, indication, event, or security incident.
 1. If the issue is an event, indication, or precursor the HIPAA Security Official forwards it to the appropriate resource for investigation.
 - a. **Physical Intrusion:** referred to the facilities manager and law enforcement.
 - b. **Non-Technical Event (minor infringement):** referred to the HIPAA Security Official completes a SIR Form and investigates the incident. If a non-technical security incident is discovered the SIRT completes the investigation, implements preventative measures, and resolves the security incident.
 - c. **Technical Event:** referred to an IT resource to assist the team in investigation, containment and resolution. Technical resources can be identified from www.sans.org, www.nist.gov or other sites.
 - d. Consideration may also be given to providing notification to the cyber-liability insurance carrier.
 2. If the issue is a security incident the HIPAA Security Official activates the Security Incident Response Team (SIRT). The SIRT is responsible for:
 - a. properly identifying an incident and the extent of the incident
 - b. providing immediate notification to appropriate parties
 - c. considering completion of a risk assessment specific to the incident
 - d. analyzing the available information
 - e. assembling the necessary SIRT members
 - f. creating an action plan and appropriate time frames
 - g. gathering data and/or evidence

1. If they have, the technical team restores the system to its proper, intended functioning (“last known good”).
 - a. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
 - b. If operation of the system(s) had been interrupted, restart the restored and validated system(s) and monitor for behavior.
 2. If the system had not been changed in any way, but was taken offline, restart the system and monitor for proper behavior.
- (b) Document all actions taken during recovery phase.
5. **Follow-up Phase (Phase V - Technical and Non-Technical):** All security incidents shall be reviewed shortly after resolution to determine where response could be improved. Timeframes may extend to one to two weeks post-incident.
 - (a) Responders to the security incident meet to review the documentation collected during the security incident.
 1. Ensure the identified corrective actions have been fully implemented.
 2. Evaluate the cost and impact of the security incident to the organization.
 3. Determine what could be improved.
 - (b) Document all actions taken during follow-up phase.
 6. **Retention of Security Incident Documentation:** Maintain all documentation surrounding every security incident, to include all work papers, notes, meeting minutes and other items relevant to the investigation in a secure location in accordance with Kewaunee County records retention schedules.