

Security Oversight Policy

Policy:

In accordance with the standards set forth in the HIPAA Security and HITECH Omnibus Rules, Kewaunee County is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI) it creates, receives, maintains, and/or transmits. To provide for the appropriate development, implementation, and oversight of Kewaunee County's efforts toward compliance of the HIPAA security regulations, Kewaunee County has a designated Security Official responsible for facilitating the training and supervision of all workforce members, investigation and sanctioning of any workforce member that is in non-compliance with the HIPAA security regulations, and writing, implementing, and maintaining all policies, procedures, and documentation related to efforts toward HIPAA security compliance.

Responsible for Implementation:

The Kewaunee County IT Director is designated as the Kewaunee County Security Official. The Security Official should work closely with the County Administrator, Human Services Director, Public Health Director and the Corporation Counsel for all issues pertaining to Kewaunee County's efforts to be compliant with the HIPAA Security Regulations.

Key Definitions:

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Workforce: Employees, volunteers, board members, community representatives, trainees, students, contractors and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Procedures:

1. **Security Official Responsibilities.** The Security Official, in collaboration with the Privacy Official, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Kewaunee County's efforts to be compliant

with the HIPAA Security Regulations. The intent of all oversight activities includes those necessary to maintain the confidentiality, integrity, and availability of ePHI. These responsibilities include, but are not limited to the following:

- (a) Oversees and enforces all activities necessary to comply with the Security rule and verifies the activities are in alignment with the requirements.
- (b) Policies and procedures
 - 1. Establishes, updates, and maintains written policies and procedures to comply with the Security rule.
 - 2. Retains them in accordance with Kewaunee County's record retention schedules.
 - 3. Provides copies of the policies and procedures to management, and has them available to review by all other workforce members to which they apply.
- (c) Periodically and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security of ePHI.
- (d) Facilitates audits to validate Security compliance efforts throughout the organization.
- (e) Documents all activities and assessments completed to comply with the Security rule.
- (f) Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
- (g) Maintains a program promoting workforce members to report non-compliance with established Security rule policies and procedures.
 - 1. Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
 - 2. Apply consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Kewaunee County.
 - 3. Mitigates to the extent practicable, any harmful effect known to Kewaunee County of a use or disclosure of ePHI in violation of Kewaunee County's and/or a business associate's policies and procedures.
- (h) Reports security efforts and incidents to administration in a timely manner.
- (i) Assists in the administration and oversight of business associates and agreements in place with them.

2. **Workforce Training.**

- (a) Official workforce training must take place upon initial hiring for each employee, biennially, and when there are changes to job function of an individual or policy and procedure changes.
- (b) Training is mandatory for all covered workforce members.
- (c) The Security Official or designee maintains documentation of the training session materials.
- (d) The training session focuses on, but is not limited to, the following subjects defined in Kewaunee County's security policies and procedures:
 - 1. Kewaunee County will monitor access and activities of all workforce members and will address any discrepancies.
 - 2. Workstations may only be used to perform assigned job responsibilities.

3. Workforce members are required to report malicious software to the Security Official or designee immediately.
 4. Workforce members are required to report unauthorized attempts, uses of, and theft of Kewaunee County's systems and/or workstations.
 5. Workforce members are required to report unauthorized access to facilities.
 6. No workforce member may alter ePHI maintained in any system, even if they have the technical ability to do so without specific authorization.
 7. Workforce members will understand that they are responsible for the security of any portable devices that they use. The level of encryption and security must correspond to the most sensitive information stored on the device. Loss or theft must be reported immediately.
 8. Workforce members are required to understand their role in Kewaunee County's contingency plan
 9. Workforce members may not share their user names nor passwords with anyone
 10. Workforce member's systems must be designed to require password change and complexity. Workforce members will be trained concerning these requirements.
 11. Workforce members must set all applications that contain or transmit ePHI to automatically log off after 5 minutes of inactivity
 12. Supervisors are required to report terminations of workforce members and other outside workforce members.
 13. Supervisors are required to report a change in a workforce member's title, role, department, and/or location
 14. Procedures to re-use or dispose of any portable media containing ePHI.
- (e) The Security Official facilitates the timely communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
1. Latest malicious software or virus alerts
 2. Kewaunee County's requirement to report unauthorized attempts to access ePHI
 3. Changes in creating or changing passwords
 4. Changes in regulatory standards
- (f) Additional training is provided to workforce members in the information services department. This training may include:
1. Data backup plans
 2. System auditing procedures
 3. Redundancy procedures
 4. Contingency plans
 5. Virus protection
 6. Media Disposal and/or Re-use
 7. Incidence response
 8. Documentation requirements

3. **Supervision of Workforce.** Although the Security Official is responsible for implementing and overseeing all activities related to compliance to the Security rule,

it is the responsibility of all leaders to supervise all workforce members, including third party vendors, contractors or other users of Kewaunee County's systems, applications, servers, workstations, etc. that contain ePHI.

- (a) Leaders monitor workstations and applications for unauthorized use, tampering, and theft.
- (b) Leaders assist the Security Official to ensure appropriate role-based access is provided to all workforce members.
- (c) Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to workforce members who comply with the Security regulation and Kewaunee County's security policies and procedures.

4. **Investigation.** All workforce members and any others with system access report non-compliance of Kewaunee County's policies and procedures to their immediate supervisor or to the Security Official. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

- (a) The Security Official promptly facilitates a thorough investigation of all reported violations of Kewaunee County's security policies and procedures. The Security Official may request the assistance from others as needed.
 - 1. Complete an audit trail/log to identify and verify the violation and sequence of events.
 - 2. Interview any individual that may be aware of or involved in the incident.
 - a. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
 - b. Provide individuals suspected of non-compliance of the Security rule and/or Kewaunee County's policies and procedures the opportunity to explain their actions.
 - 3. The designated investigators thoroughly document the investigation in a timely manner.
 - 4. The Security Official facilitates taking appropriate steps to prevent recurrence of the violation.