

Risk Management Policy

Purpose:

This policy establishes the scope, objectives, and procedures of Kewaunee County's information security risk management process. The risk management process is intended to support and protect the Kewaunee County and its ability to fulfill its mission.

Policy:

1. It is the policy of Kewaunee County to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information (ePHI) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the Kewaunee County's information security program.
2. Risk analysis and risk management are recognized as important components of Kewaunee County's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule.
 - (a) Risk assessments are done throughout IT system life cycles:
 - i. Before the purchase or integration of new technologies and changes are made to physical safeguards;
 - ii. While integrating technology and making physical security changes; and
 - iii. While sustaining and monitoring of appropriate security controls.
 - (b) The Kewaunee County performs periodic technical and non-technical assessments of the security rule requirements as well as in response to environmental or operational changes affecting the security of ePHI.
3. Kewaunee County implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
 - (a) Ensure the confidentiality, integrity, and availability of all ePHI the Kewaunee County creates, receives, maintains, and/or transmits,
 - (b) Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI,
 - (c) Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and
 - (d) Ensure compliance by workforce.
4. All Kewaunee County workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to Kewaunee County's Sanction policy.
5. All risk management efforts are documented and the documentation.

Scope

The scope of the information security risk management process covers the administrative, physical, and technical processes that enable and govern ePHI that is received, created, maintained or transmitted.

Key Definitions:

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

Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets.

Risk Management Team: Individuals who are knowledgeable about Kewaunee County's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.

Risk Assessment: (Referred to as *Risk Analysis* in the HIPAA Security Rule); the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an Kewaunee County given its mission and available resources.

Threat: the potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:

- Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Threat Source – Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the Kewaunee County 's ability to protect ePHI.

Threat Action – The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Procedures:

1. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Kewaunee County's Security Officer and the Risk Management Team.
2. **Risk Assessment:** The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.
 - (a) Step 1. System Characterization
 - i. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices.
 - ii. *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.
 - (b) Step 2. Threat Identification
 - i. In this step, potential threats are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from all available sources. The list should be based on Kewaunee County individual characteristics and its processing environment.
 - ii. *Output* – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.
 - (c) Step 3. Vulnerability Identification
 - i. The goal of this step is to develop a list of technical and non-technical system vulnerabilities that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern Kewaunee County's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software,

hardware, or other deficiencies that comprise Kewaunee County’s computer network.

- ii. *Output* – A list of the system vulnerabilities that could be exercised by the potential threat-sources.

(d) Step 4. Control Analysis

- i. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the Kewaunee County to minimize or eliminate the likelihood of a threat-source exploiting a system vulnerability.
- ii. *Output* – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

(e) Step 5. Likelihood Determination

- i. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.
- ii. *Output* – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Likelihood Definition	
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

(f) Step 6. Impact Analysis

- i. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the Kewaunee County’s mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data. (See “Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions”.)
- ii. *Output* – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Impact Definition	
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm,

	or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably

(g) Step 7. Risk Determination

- i. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised.
- ii. *Output* – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

Risk Description and Necessary Actions	
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system’s DAA must determine whether corrective actions are still required or decide to accept the risk.

(h) Step 8. Control Recommendations

- i. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to Kewaunee County’s operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options legislation and regulation, Kewaunee County policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
- ii. *Output* – Recommendation of control(s) and alternative solutions to mitigate risk.

(i) Step 9. Results Documentation

- i. Results of the risk assessment are documented in an official report or briefing and provided to the County Administrator to make decisions on policy, procedure, budget, and system operational and management changes.

- ii. *Output* – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.
3. **Risk Mitigation:** Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the Kewaunee County consistent with its goals and mission.
- (a) Step 1. Prioritize Actions –
 - i. Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources
 - ii. *Output* – Actions ranked from high to low
 - (b) Step 2. Evaluate Recommended Control Options –
 - i. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
 - ii. *Output* – list of feasible controls
 - (c) Step 3. Conduct Cost-Benefit Analysis –
 - i. Determine the extent to which a control is cost-effective. Compare the benefit of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.
 - ii. *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific control
 - (d) Step 4. Select Control(s) –
 - i. Taking into account the information and results from previous steps, the Kewaunee County’s mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.
 - ii. *Output* – Selected control(s)

- (e) Step 5. Assign Responsibility –
 - i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.
 - ii. *Output* – List of resources, responsible persons and their assignments

- (f) Step 6. Develop Safeguard Implementation Plan –
 - i. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
 - a. Each risk or vulnerability/threat pair and risk level
 - b. Prioritized actions
 - c. The recommended feasible control(s) for each identified risk
 - d. Required resources for implementation of selected controls
 - e. Team member responsible for implementation of each control
 - f. Start date for implementation
 - g. Target date for completion of implementation
 - h. Maintenance requirements.
 - ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the Kewaunee County Administrator and Board.
 - iii. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations. Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates and project requirements.
 - iv. *Output* – Safeguard Implementation Plan

- (g) Step 7. Implement Selected Controls – as controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risk is not practical. Depending on individual situations, implemented controls may lower a risk level but not completely eliminate the risk.
 - i. Continually and consistently communicate expectations to all Risk Management Team members and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

- ii. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.
 - iii. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.
 - iv. *Output* – Residual Risk
4. **Risk Management Schedule:** The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of Kewaunee County's information security program:
- (a) Scheduled Basis – an overall risk assessment of Kewaunee County's information system infrastructure will be conducted biennially. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the budgeting process.
 - (b) Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
 - (c) As Needed – the Security Officer or Risk Management Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect Kewaunee County's information systems.
5. **Process Documentation.** Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for a minimum of six years.