

Information System Activity Review Policy

Policy:

Kewaunee County shall review logs of access and activity of electronic protected health information (ePHI) applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI. The Security Rule requires healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Kewaunee County shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to reviewing of logs which is consistent with available resources.

Responsible for Implementation:

- Security Official
- Privacy Official
- Administration

Applicable To:

- All Workforce Members
- Organization's Business Associates

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:

It is the policy of Kewaunee County to safeguard the confidentiality, integrity, and availability of patient health information applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, Kewaunee County shall review logs of access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions.
- Breaches in confidentiality and security of patient protected health information.
- Performance problems and flaws in applications.
- Improper alteration or destruction of ePHI (information integrity).

This policy applies to organizational information applications, systems, networks, and any computing devices, regardless of ownership.

Scope:

This policy has been developed to address the organization-wide approach to information system log review processes. Departments shall work with the Security Official to develop specific procedures based on applications and systems for review processes.

Key Definitions:

Log Review: The internal process of reviewing information system access and activity. A review may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing. Review activities shall also take into consideration Kewaunee County information system risk analysis results.

System Logs: Records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity; 3) identification of user performing activity; and 4) description of attempted or completed activity.

Review Trail: A means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities. Review trails provide:

- Individual accountability for activities such as an unauthorized access of ePHI;
- Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information;
- Problem analysis such as an investigation into a slowdown in a system's performance, and
- Other data as needed based on Kewaunee County's objectives

*A review trail identifies **who** (login) did **what** (create, read, modify, delete, add, etc.) to **what** (data) and **when** (date, time).*

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

Trigger Event: Activities that may be indicative of a security breach that require further investigation.

Procedures:

General

1. Responsibility for reviewing information system access and activity is assigned to Kewaunee County Information Systems (IS) Department Head or other designee as determined by the Kewaunee County Administrator. The responsible individual shall:
 - (a) Assign the task of generating reports for review activities to the individual responsible for the application, system, or network.
 - (b) Assign the task of reviewing the logs to the individual responsible for the application, system, or network, the Privacy Official, or any other individual determined to be appropriate for the task.

- (c) Organize and provide oversight to a team structure charged with review compliance activities.
2. Kewaunee County reviewing processes shall address access and activity at the following levels listed below. Reviewing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
 - (a) User: User level review trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and files, patients, and resources accessed.
 - (b) Application: Application level review trails generally monitor and log user activities, including data files opened and closed, patients accessed, specific actions, and printing reports.
 - (c) System: System level review trails generally monitor and log user activities, applications accessed, and other system defined specific actions.
 - (d) Network: Network level review trails generally monitor information on current operations, penetrations, and vulnerabilities.
3. Kewaunee County shall determine the systems or activities that will be tracked or reviewed by:
 - (a) Focusing efforts on areas of greatest risk and vulnerability as identified in the information systems risk analysis and ongoing risk management processes.
 - (b) Maintaining confidentiality, integrity, and availability of ePHI applications and systems.
 - (c) Assessing the appropriate scope of system reviews based on the size and needs of Kewaunee County by determining:
 - i. information/ePHI at risk,
 - ii. systems, applications or processes which are vulnerable to unauthorized or inappropriate access,
 - iii. activities that should be monitored (create, read, update, delete = CRUD),
 - iv. information to be included in the review record.
 - (d) Assessing available organizational resources.
4. Kewaunee County shall identify “trigger events” or criteria that raise awareness of questionable conditions of viewing of confidential information. The “events” may be applied to the entire organization or may be specific to a department, unit, or application. At a minimum, Kewaunee County shall provide immediate reviewing in response to:
 - (a) Patient complaint.
 - (b) Employee complaint.
 - (c) Suspected breach of patient confidentiality.
 - (d) High risk or problem prone event.
 - (e) External report, such as from credit bureau or law enforcement.
5. Kewaunee County shall determine review criteria with a risk based approach. This may include but is not limited to reviewing security risk analysis findings, past experience, current and projected future needs, and industry trends and events. Kewaunee County will determine its ability to generate, review, and respond to

review reports using internal resources. Kewaunee County may determine that external resources are also appropriate. Kewaunee County recognizes that failure to address automatically generated review logs, trails, and reports through a systematic review process may be more detrimental to the organization than not reviewing at all.

6. Kewaunee County shall designate the employees or contractors who are authorized to use security testing and monitoring tools. Such tools may not be used by anyone not specifically authorized. These tools may include, but are not limited to:
 - A. Scanning tools and devices.
 - B. War driving software.
 - C. Password cracking utilities.
 - D. Network or wireless packet capture utilities.
 - E. Passive and active intrusion detection systems.
 - F. Other devices as determined by Kewaunee County.
7. Review documentation/reporting tools shall address, at a minimum, the following data elements:
 - A. Authorizing official or policy, Application, System, Network, Department, and/or User Reviewed.
 - B. Review Type.
 - C. Individual/Department Responsible for Review.
 - D. Date(s) of Review.
 - E. Reporting Responsibility/Structure for Review Results.
 - F. Conclusions.
 - G. Recommendations.
 - H. Actions.
 - I. Assignments.
 - J. Follow-up.
8. The process for review of logs, trails, and reports shall include:
 - A. Description of the activity as well as rationale for performing review.
 - B. Identification of which workforce members or department/unit will be responsible for review.
 - C. Frequency of the reviewing process.
 - D. Determination of significant events requiring further review and follow-up.
 - E. Identification of appropriate reporting channels for review of results and required follow-up.
9. Vulnerability testing software may be used to probe the network. This may be to identify what is running. Any publicly-known vulnerabilities should be corrected. Re-evaluate whether the system can withstand attacks aimed at circumventing security controls.
 - A. Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party reviewing vendor should not be providing the organization IT oversight services.
 - B. Testing shall be done on a biennial basis.

Review Requests for Specific Cause

1. A request may be made for review for a specific cause. The request may come from a variety of sources including, but not limited to, a patient, the County Administrator, Privacy Official, or Security Official.

2. A request for a review for specific cause must include time frame and nature of the request. The request must be reviewed and approved by Kewaunee County Privacy or Security Official.
3. A request for a review as a result of a patient concern shall be initiated by Kewaunee County Privacy Official and/or Security Official. Detailed review may be shared with patient. If this is done, a careful explanation must be given to the patient concerning the need for many individuals to have access to records.
 - A. Should the review disclose that a workforce member has accessed a patient's PHI inappropriately, the information shall be shared with the workforce member's supervisor/and or County Administrator to determine appropriate sanction/corrective disciplinary action.
 - B. Kewaunee County may, but is not obligated to share details of the logs with the patient. Prior to communicating with the patient, consider the need to collaborate with risk management and/or legal counsel for incidents of a more sensitive nature.

Evaluation and Reporting of Review Findings

1. System logs that are routinely gathered must be reviewed in a timely manner.
2. Report of review of results shall be limited on a minimum necessary/need to know basis. Review of results may be disclosed as deemed necessary. Legal or administrative counsel may need to be consulted.
3. There is no legal requirement to disclose the name of an individual who breached a patient's record. There is also no obligation to share the name of every individual that was involved in processing a patient record. Kewaunee County may choose to disclose this information. If the organization chooses to provide a complete list of everyone that accessed a record, it must be done with a careful explanation to the patient. Most patients do not know how many individuals are involved in processing their records. When a patient asks if a specific individual has accessed records, only that name should be disclosed.
4. The reporting process shall allow for meaningful communication of the review findings to the appropriate departments/units.
 - A. Significant findings shall be reported immediately in a written format.
 - B. Routine findings shall be reported to the sponsoring leadership structure in a written report format.
5. Security reviews constitute an internal, confidential monitoring practice that may be included in Kewaunee County performance improvement activities and reporting. Care shall be taken when releasing the results of the reviews. Review information which may further expose organizational risk should be shared with extreme caution. Generic security review information may be included in organizational reports (PHI shall not be included in the reports).
6. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible and sponsoring departments/units.
7. If criminal activity is discovered during a review, it should be reported to appropriate law enforcement agency.

Reviewing Business Associate and/or Vendor Access and Activity

1. Periodic monitoring of business associate and vendor information system activity should be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between Kewaunee County and the external agency.
2. If it is determined that the business associate or vendor has exceeded the scope of access privileges, Kewaunee County leadership must reassess the business relationship.
3. If it is determined that a business associate has violated the terms of the HIPAA business associate agreement, Kewaunee County must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Review Log Security Controls and Backup

1. Review logs shall be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident.
2. Whenever possible, audit trail information shall be stored on a separate system. This is done to apply the security principle of “separation of duties” to protect audit trails from hackers. Audit trails maintained on a separate system would not be available to hackers who may break into the network and obtain system administrator privileges. A separate system would allow Kewaunee County to detect hacking security incidents.
3. Review logs maintained within an application shall be backed-up as part of the application’s regular backup procedure.
4. Kewaunee County shall review internal back-up, storage and data recovery processes to ensure that the information is readily available in the manner required.

Workforce Training, Education, Awareness and Responsibilities

1. Kewaunee County workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and patient protected health information. Kewaunee County commitment to reviewing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the reviewing process detect a workforce member’s failure to comply with organizational policies.

External Reviews of Information Access and Activity

1. Information system review information and reports gathered from contracted external review firms, business associates and vendors shall be evaluated and appropriate corrective action steps taken as indicated. Prior to contracting with an external review firm, Kewaunee County shall:
 - A. Outline the review responsibility, authority, and accountability.
 - B. Choose a review firm that is independent of other organizational operations.
 - C. Ensure technical competence of the review firm staff.
 - D. Require the review firm’s adherence to applicable codes of professional ethics.
 - E. Obtain a signed HIPAA-compliant business associate agreement.

F. Assign organizational responsibility for supervision of the external review firm.

Retention of Review Information

1. Review logs and audit trail report information shall be maintained based on Kewaunee County's retention of records schedule.