Kansas Health Information Network, Inc. d/b/a KONZA

Privacy & Security

Policy and Procedure Manual

The Kansas Health Information Network, Inc. (KHIN) d/b/a KONZA policies and procedures apply to all of the organizations that KHIN does business as (d/b/a) in other states. In 2024 this includes KHIN (Kansas), Carolina eHealth Network (South Carolina), CTHealthLink (Connecticut), HealtheParadigm (Georgia), HealthSYNC (Louisiana), GenesisLink (Texas), OneHealth New Jersey (New Jersey), SHINE (Missouri), MHAX (Mississippi), and KONZA HIE.

Contents

SECTION ONE – WORKFORCE POLICIES

Governance of the Privacy & Security Information Protection Program	
Kansas Health Information Network, Inc. ***Policies & Procedures***	Policy #: 001
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Applicability of Federal HIPAA Regulations to Kansas Health Information Network, Inc.:

Responsibility: HIPAA Risk and Security Committee

Policy:

Kansas Health Information Network, Inc. has established a comprehensive Privacy and Security Information Protection Program ("Program"). The Program employs a continuous monitoring strategy and utilizes continues monitoring across all the defined controls. A critical component of the Program is the HIPAA Risk and Security Committee comprised of a Privacy Security Officer (PSO), Chief Operating Officer and the President. This committee functions to assure the initial implementation and ongoing monitoring of KONZ's compliance with federal requirements in this area.

Responsibilities

1. The HIPAA Risk and Security Committee is accountable for:

1.1. The general administrative oversight and compliance monitoring of the business associate's ability to meet privacy, cyber security, and security requirements.

1.1.1. Oversight includes assuring the adequate and applicable resources are allocated to continue ongoing privacy/security compliance including but not limited to capital resource and financial planning.

1.1.1.1. Job descriptions define roles and responsibilities are defined in writing and clearly communicated to job candidates.

1.1.2. The program and all policies, procedures and technical controls are in alignment with continuous monitoring strategy, relevant regulation/legislation, industry standard framework, business requirements and revised as necessary to continue ongoing compliance.

1.1.2.1. Independent audits are conducted on an annual basis, results are reviewed, appropriately mitigated, and approved with a summary report to the senior leadership team and communicated by the executive management to all stakeholders.

1.1.2.2. Receive regular reports from the Security Team on potential vulnerabilities.

1.1.2.3. Assess potential vulnerabilities, focusing on risk ratings, risk tolerance, and mitigation plans.

1.1.2.4. Define, maintain, and update organizational policies to ensure the Organization's ability to meet privacy, cyber security, and security requirements.

1.1.3. Information Privacy and Security principles, importance, objectives, scope/goals and related documents are formally identified, prioritized, and communicated to all workforce members in a manner that is user friendly and understandable.

1.1.4. Information security and privacy best practices are addressed in all phases of project management methodology and software development lifecycle.

1.1.4.1. Kansas Health Information Network, Inc. includes business requirements for the availability of information systems when specifying the security requirements; and, where availability cannot be guaranteed using existing architectures, redundant components or architectures are considered along with the risks associated with implementing such redundancies.

1.1.4.2. The requirement definition phase includes (i) consideration of system requirements for information security and the processes for implementing security, and (ii) data classification and risk to information assets are assigned and approved (signed-off) by management to ensure appropriate controls are considered and the correct project team members are involved.

1.1.4.3. Kansas Health Information Network, Inc. develops enterprise architecture with consideration for information security and the resulting risk to operations, assets, and individuals, as well as other organizations.

1.1.4.4. Kansas Health Information Network, Inc. has developed an information security architecture for the information system.

1.1.4.5. Kansas Health Information Network, Inc. reviews and updates (as necessary) the information security architecture whenever changes are made to the enterprise architecture and ensures that planned information security architecture changes are reflected in the security plan and organizational procurements and acquisitions.

1.1.5. Actions that can be performed without identification and authentication are only allowed by written exception from the HIPAA Risk and Security Committee.

1.1.6. The responsibility to convene, investigate, mitigate, and resolve any potential security incidents or data breach.

1.1.7. Assure the contracted relationship between Kansas Health Information Network, Inc. and its HIPAA covered entity client/health plans are carried out as defined.

1.1.8. To meet regularly throughout each calendar year to address ongoing findings and compliance status.

1.1.8.1. Detailed minutes of such meetings (and progress notes on action items) are clearly documented and maintained with compliance documentation by the Privacy & Security Officer. Such compliance documentation will be retained by Kansas Health Information Network, Inc. for as long as it is applicable, plus six years.

Designation of HIPAA Officials	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 002
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO)

Policy:

Chief Information Security Officer

The Kansas Health Information Network, Inc. Board of Directors has designated a focused role to develop, implement, and monitor a strategic, comprehensive Privacy & Security Information Protection Program. Essential functions include:

1. Ensure that processes needed for the Information Security Management System (ISMS) are established, implemented, and maintained in accordance with the standard requirements.
2. Ensuring the promotion of awareness of customer, legal, and Information security requirements are communicated to employees and contractors.
3. Liaison with external bodies regarding Privacy & Security Information Protection Program.
4. Appraisal on the performance of the Privacy & Security Information Protection Program system regarding the needs for improvement to the Management.
5. Conducting Internal audits and review meetings.
6. Following procedures to Control Documents and Records.

Director of Privacy and Data Compliance

The Kansas Health Information Network, Inc. Board of Directors has designated a Director of Privacy and Data Compliance as a focused role to oversee the Organization's privacy policies and procedures and federal privacy regulations [45 CFR § 164.530(a)(1)] along with the Organization's security policies and procedures and federal security regulations [45 CFR § 164.308(a)(2)].

The Kansas Health Information Network, Inc. Board of Directors has designated the Director of Privacy and Data Compliance (DPDC) as the contact person to receive complaints, requests for access to PHI, to amend PHI, or for an accounting for disclosures of PHI regarding the privacy of *protected health information*, or to receive other information regarding the Privacy and Security policies and procedures.

Procedures:

Retention Period

This record of designations will be retained for as long as the designations are in effect, and for a period of six years after it is superseded by a subsequent designation.

General Guidelines to Safeguard Protected Health information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 003
Section: ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.530(c)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

Kansas Health Information Network, Inc. will use reasonable administrative, physical, and technical safeguards to protect the privacy of protected health information and limit incidental uses or disclosures of protected health information. An incidental *use* or *disclosure* is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard.

All members of the Kansas Health Information Network, Inc. workforce will follow these guidelines in handling protected health information (PHI) in order to protect the privacy of protected health information, limit incidental uses and disclosures and ensure cyber security and general security controls are in place.

GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION

1. Physical or remote company share location:

    1.1. Bulletin boards or remote company share locations may not contain any documents with PHI of members, unless the member has authorized the display in accordance with the Authorization to use or Disclose Protected Health Information Privacy Policy. This includes:

    - Baby pictures (even without a name or other identifying information)
    - Cards and notes of appreciation

2. Cleaning personnel:

    2.1. Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets, or rooms before cleaning personnel enter an area.

3. Computer Monitors/Screens:

    3.1. Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed.

    3.2. Computer displays will be configured to go blank, or to display a screen saver when left unattended for more than a brief period of time. The Director of Privacy and Data Compliance (DPDC) will determine the period of time. Wherever practicable, reverting from the screen saver to the display of data will require a password.

    3.3. Computer screens left unattended for longer periods of time will log off the user. The Director of Privacy and Data Compliance (DPDC) will determine the period of time.

3.4. For procedures regarding use of email and social media See email and Protected Health Information.

4. Conversations:

4.1. Conversations concerning members' claims or other PHI must be conducted in a way that reduces the likelihood of being overheard by others.

5. Handling Data/Copying claims and other PHI:

5.1. When PHI is copied/imaged printed, only the information that is necessary to accomplish the purpose for which the copy is being made, may be prepared. This may require that part of a page be masked.

5.2. Copy (including print screen), print, move, storage of PHI is prohibited when remotely accessed without a defined business need.

5.3. Hard copy PHI is to be protected when using internal or external mail services such as USPS.

6. Desks and countertops:

6.1. Claims and other medical record documents that contain PHI must be placed face down on counters, desks and other public places where third parties can see them.

6.2. Wherever it is reasonably possible to do so, claims and other documents containing PHI will not be left on desks and countertops after business hours or for extended periods of time unsupervised. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area is left unattended.

6.3. In areas where locked storage after hours cannot reasonably be accomplished, PHI must be kept out of sight. A supervisor must be present whenever someone who is not authorized to have access to that data is in the area.

7. Disposal of paper with PHI:

7.1. Paper documents containing PHI must be shredded when no longer needed. If retained for a commercial shredder, they must be kept in a locked bin. Each department within Kansas Health Information Network, Inc. that generates any hard copy PHI (i.e., regular sized paper, or sticky notes) must be trained and routinely measured to ensure compliance with this requirement. PHI must be rendered unusable, unreadable or indecipherable to unauthorized individuals before it can be considered disposed of properly. Workforce members are to be held accountable to follow specific instructions on such disposal processes and to report as an incident any instance that PHI is found on hard copy that is not appropriately safeguarded. Sanctions are to be invoked against any workforce members who fail to dispose of hard copy PHI according to Kansas Health Information Network, Inc. policies and procedures. Records of such breaches are to be reported to Senior Management on a routine basis in aggregate form and trigger ongoing risk management analysis as appropriate.

8. Teleworking/Home office:

8.1. Any member of the workforce who is authorized to work from a home office must assure that the home office complies with all applicable policies and procedures including but not limited to physical security, general workspace and technical controls regarding the security and privacy of PHI, including these guidelines. In addition, the Remote Workforce Checklist and Guidelines on Teleworking are to be reviewed and completed prior to beginning home office work. The review of this checklist is also considered specific training as it includes the risks, controls implemented and workforce member responsibilities. Completion and approval of the Remote Workforce Checklist assures that suitable protections are in place to protect against unauthorized access, disclosure of PHI and/or theft of equipment and data.

8.2. Once the Remote Workforce Checklist is completed and if approved, the workforce member's Manager is responsible to document the permitted level of work to be conducted including classification of PHI that may be handled/stored, standard operating hours, defined systems/services for permitted access, review of equipment and storage furniture and clarity on use of private equipment. Additionally, guidance on handling visitors/family access to the workspace, cyber security threats, technical maintenance of equipment/systems and business continuity planning should be included.

9. Protection of information when traveling:

9.1. When a member of the workforce is traveling, PHI or devices that contain PHI may not be left unattended unless it is in a locked vehicle, in an opaque, locked container. Locking the vehicle alone is not sufficient.

9.2. Information (data) stored on removable media should be encrypted and/or password protected. Removable media should be carried separately from laptop or mobile device (when possible, keep jump-drives and other removable media separate from the laptop or other mobile device). All passwords, login instructions and authentication tools should be kept separate from the laptop or mobile device. Consider using screen protectors as a method to discourage shoulder surfing.

9.3. Backup your laptop/device data on a regular basis by copying data to encrypted removable media or by uploading critical files to a non-shared drive on a Kansas Health Information Network, Inc. managed server. Protect the backup media appropriately. If the data that you are backing up is confidential, personal, and/or sensitive use special precautions to ensure that it is handled appropriately.

9.4. Be wary of using mobile devices (laptops, Company mobile phones, and/or tablets) public places. Keep conversations low and be aware of others attempting to overhear or shoulder surfing (attempting to see passwords and other private information). Consider using screen protectors as appropriate to discourage shoulder surfing. Do not download information onto hotel computers.

9.5. When travelling to high-risk locations, specially configured mobile devices may be issued and checked for physical tampering and malware upon their return to the office.

10. Company mobile phones:

10.1. Kansas Health Information Network, Inc. privacy and security policies apply to any PHI that is stored on a Company mobile phones.

10.2. Users of Company mobile phones are responsible for assuring that the PHI on their devices is kept secure and private.

10.3. Any loss or theft of a company mobile phones thought to contain PHI must be reported to the Security Official immediately.

10.4. Users of Company mobile phones who store PHI on their devices will receive special training in the risks of this practice, and measures that they can take to reduce the risks (such as use of passwords, token devices, or biometrics).

10.5. At termination of employment, users of Company mobile phones will return the device as part of offboarding.

11. Printers:

11.1. Printers must be located in secure areas, where only authorized members of the workforce can have access to documents being printed.

12. Record Storage:

12.1. Areas where claim and medical records and other documents that contain PHI are stored must be secure.

12.1.1. Wherever reasonably possible, the PHI will be stored in locking cabinets or a records room. A records room is a restricted secure area which can be locked, and access is controlled.

12.1.2. Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision.

13. Subsidiary databases:

13.1. Any member of the Kansas Health Information Network, Inc. workforce who maintains a separate database which contains PHI must have a documented exception from the HIPAA Risk and Security Committee.

13.2. The Director of Privacy and Data Compliance (DPDC) must determine whether this database constitutes a "designated record set."

14. Physical Facility Controls and Safeguards: Kansas Health Information Network, Inc. does not currently maintain a physical facility. Policies are maintained in the event this changes.

14.1. Cleaning personnel:

14.2. Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets, or rooms before cleaning personnel enter an area.

14.3. Record Storage:

14.3.1. Areas where claim and medical records and other documents that contain PHI are stored must be secure.

14.3.2. Wherever reasonably possible, the PHI will be stored in locking cabinets or a records room. A records room is a restricted secure area which can be locked, and access is controlled.

14.3.3. Where locking cabinets are not available, the storage area must be locked when no member of the workforce is present to observe who enters and leaves and no unauthorized personnel may be left alone in such areas without supervision.

14.4. Key /Badge policy:

14.4.1. The Director of Privacy and Data Compliance (DPDC) will develop a list by job title of personnel who may have access to which keys. This includes electronic key cards (swipe cards) and metal keys, and applies to keys to storage cabinets, storage rooms, secure areas, and buildings.

14.4.2. All keys must be signed out.

14.4.3. Keys must be surrendered upon termination of employment.

14.4.4. The Director of Privacy and Data Compliance (DPDC) will change locks whenever there is evidence that a key is no longer under the control of an authorized member of the workforce, and its loss presents a security threat that justifies the expense.

14.5. Visible identification is to be worn by all workforce members including employees, visitors, third parties and contractors.

14.6. The authorization and validation of access is managed with physical authentication controls.

14.7. A list or audit trail of physical access is maintained for at least two years and visitor activity is reviewed monthly.

14.8. Adequate fire prevention (detectors) and suppression equipment (fire extinguishers) is in place throughout the physical facility. Workforce members are trained as applicable on use of and maintenance of the equipment. Automatic notification to fire authorities when an alarm is activated occurs.

14.9. The Director of Privacy and Data Compliance (DPDC) must assure that the data is secure, and in compliance with relevant Kansas Health Information Network, Inc. policies.

14.10. If the data is to be synchronized with other databases additional procedures must be in place to ensure integrity.

14.11. Any member of the workforce who uses and discloses PHI in a subsidiary database must follow Kansas Health Information Network, Inc. policies.

15. Workforce Vigilance:

15.1. All members of the workforce have a responsibility to watch for unauthorized use or disclosure of PHI, to act to prevent the action, and to report suspected breaches of privacy, cyber security and security policies to their supervisor, or to the DPDC Director of Privacy and Data Compliance (DPDC) (example of a breach: member or visitor looking through a claim left on a desk). This includes wearing visible identification at all times, preventing "piggybacking" upon entrance points to the physical building and use of authentication controls to authorize and validate access.

15.2. This responsibility will be included in workforce training.

15.3. This responsibility is documented in applicable job descriptions.

16. Visitors:

17.1. All visitors are granted only specific access and must sign in and out of Kansas Health Information Network, Inc. office buildings. A member of the Kansas Health Information Network, Inc. workforce must accompany all visitors to any area where PHI is stored or in use. Instructions should be provided regarding security requirements and emergency procedures.

General Policy - Use and Disclosure of Protected Health Information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 004
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.506*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

Kansas Health Information Network, Inc., when functioning as a BA, is committed to protect the privacy of the CE's health information, and to comply with applicable federal and state laws that protect the privacy and security of the entity's health information. This policy establishes the basic requirements for the use or disclosure of the CE's protected health information, consistent with this commitment.
This policy is subject to:

1. "Minimum Necessary Rule".
2. CE's Notice of Privacy Practices.
3. Limitations imposed by the "Use or Disclosure of Psychotherapy Notes" policy.
4. Any restrictions on the use or disclosure of PHI to which Kansas Health Information Network, Inc. has agreed (see "Requests to Restrict the Use or Disclosure of Protected Health Information" policy).

Workers may use and disclose protected health information, without the written consent or authorization of the person to whom the information pertains, as follows:

1. Workers may use PHI:
   - 1.1. To provide treatment.
   - 1.2. To obtain payment.
   - 1.3. For health care operations.
2. Workers may disclose PHI to providers of health care for treatment of the individual to whom the PHI pertains. The Minimum Necessary Rule does not apply to such disclosures.
3. Workers may disclose PHI:
   - 3.1. For treatment (the Minimum Necessary Rule applies if the disclosure is not to a health care provider).
   - 3.2. To obtain payment.
   - 3.3. To BAs, under the terms of a business associate agreement (BAA) for any purpose for which the BA may use the information as allowed by its contract or agreement with the CE. (see ***Determination of Relationship between CEs & Kansas Health Information Network, Inc.*** **and** ***Disclosure of PHI to 2nd Tier Business Associates of Kansas Health Information Network, Inc.***).
   - 3.4. To other CEs that participate in an organized health care arrangement with the CE, to the extent those entities need the PHI for purposes of their own payment and health care operations.

3.5. To other CEs that do not participate with the CE in an organized health care arrangement, for purposes of:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities ("obtaining generalizable knowledge" means conducting research);
- Conducting population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and related functions that do not include treatment;
- Contacting of health care providers and patients / health plan members with information about treatment alternatives;
- Reviewing the competence or qualifications of health care professionals;
- Evaluating practitioner, provider and health plan performance;
- Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers;
- Training of non-health care professionals;
- Accreditation, certification, licensing, or credentialing activities;
- Health care fraud and abuse detection or compliance;
- PHI may ONLY be disclosed to a CE that does not participate with another CE in an organized health care arrangement, for the purposes listed in the above paragraph, if both the CE and the receiving entity has or had a relationship with the patient / health plan member, and the information that is disclosed pertains to this relationship.

4. Workers may <u>disclose</u> PHI in accordance with each of the following Kansas Health Information Network, Inc. policies:

4.1. Verification of The Identity and Authority of a Person Requesting Disclosure of Protected Health Information.

4.2. Disclosures of Protected Health Information That Are Required by Law – General Policy.

4.3. Disclosure of Protected Health Information for Public Health Purposes.

4.4. Disclosure of Protected Health Information to Report Child Abuse, Or Other Abuse, Neglect, Or Domestic Violence.

4.5. Disclosure of Protected Health Information To "Regulators".

4.6. Disclosure of Protected Health Information in Disaster Situations.

4.7. Disclosure of Protected Health Information Without Authorization, To Avert A Serious Threat to Health or Safety.

4.8. Disclosure of Protected Health Information to Personal Representatives.

4.9. Right of Access to Protected Health Information.

5. Workers may <u>use and disclose</u> PHI in accordance with each of the following Kansas Health Information Network, Inc. policies:

5.1. Extension of Privacy Protection to Deceased Individuals.

5.2. Authorization to Use or Disclose Protected Health Information.

5.3. De-Identified Information (relating to the use and disclosure of PHI for the purpose of de-identifying it).

5.4. Limited Data Set.

5.5. Use and Disclosure of Protected Health Information for Purposes of Research.

5.6. Use or Disclosure of Psychotherapy Notes.

6. Protected health information does not include (and this policy does not apply to):

6.1. Records covered by the Family Educational Right and Privacy Act.

6.2. Employment records held by the Covered Entity in its role as employer.

6.3. NOTE: Proposed Rule Making also adds "Regarding a person who has been deceased for more than 50 years".

Procedures:

Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) is required to:

1. Ensure that all members of Kansas Health Information Network, Inc.'s workforce and subcontractors are thoroughly trained in the uses and disclosures of PHI that are permitted by this policy.

1.1. Consider using Sample Notice of Privacy Practices as training tool for Uses and Disclosures of PHI.

2. Ensure that all applicable Kansas Health Information Network, Inc. workforce members and subcontractors are thoroughly trained in the provisions of the contracted Covered Entity's policies that govern the use and disclosure of PHI.

Minimum Necessary Rule	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 005
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.502(b), 164.514(d)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

1. When providing services as a BA, members of the Kansas Health Information Network, Inc.'s workforce, including subcontractors and agents, may not use, request, or disclose to others, any PHI that is more than the minimum necessary to accomplish the purpose of the use, request, or disclosure.
2. Members of the workforce, including subcontractors and agents, are required to comply with specific policies and procedures established to limit uses of, requests for, or disclosures of PHI to the minimum amount necessary.
3. Kansas Health Information Network, Inc.'s workers, subcontractors and agents may not use, disclose, or request an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.
4. If the CE has approved the disclosure and if such reliance is reasonable under the circumstances, Kansas Health Information Network, Inc. may rely on a request for PHI as representing the minimum necessary for the stated purpose in the following situations:
    4.1. The request is from a public official.
        4.1.1. The disclosure to the public official must otherwise be permitted under Kansas Health Information Network, Inc.'s policies, and
        4.1.2. The public official must represent that the information requested is the minimum necessary for the stated purpose(s); or,
    4.2. The information is requested by another CE; or,
    4.3. The information is requested by a professional who is a member of the CE's workforce or is another BA of the CE, and
        4.3.1. The purpose of the request is to provide professional services to the CE, and
        4.3.2. The professional represents that the information requested is the minimum necessary for the stated purpose(s); or,
    4.4. The request is for research purposes, and the requestor has complied with the CE's policy regarding disclosure of PHI for research and has presented all documentation or representation required by that policy.

Exceptions:
When a disclosure has been approved by the CE:

1. Kansas Health Information Network, Inc. is not limited in the amount of PHI that it may disclose to a provider of health care <u>for the purpose of medical treatment</u>. Nor is Kansas Health Information

Network, Inc. limited in the amount of PHI that it may request, from any source, for the purpose of payment when Kansas Health Information Network, Inc. is acting on behalf of a CE for such purpose.

2. When federal or state law requires a disclosure of PHI, the minimum necessary amount of information is that which is required in order to comply with such law. Requests for PHI made by the federal government in the course of a complaint investigation or compliance review, undertaken under federal privacy rules, are deemed to meet the minimum necessary rule.
3. When disclosing a patient's or health plan member's own information to that patient or health plan member, or to the personal representative, the minimum necessary rule does not apply.
4. All information that is requested by an authorization may be disclosed in accordance with that authorization. This policy does not limit such disclosures.
5. Kansas Health Information Network, Inc. may request, use, and disclose all required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions, in connection with conducting HIPAA standard transactions.

Duty to Report Security or Privacy Breach and Mitigate the Effect	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 006
Section: ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.530(f)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO), Workforce

Policy:

1. It is the duty of all members of the *workforce or subcontractors* to report any unauthorized acquisition, access, use or disclosure of PHI or other breach of Kansas Health Information Network, Inc. privacy and security policies immediately to the Kansas Health Information Network, Inc. President and/or Privacy & Security Officer.
2. Upon becoming aware of the potential breach, the Kansas Health Information Network, Inc. HIPAA Risk and Security Committee will promptly investigate any alleged breach of the privacy or security of protected health information (PHI).
3. Using this policy and procedure the Kansas Health Information Network, Inc. HIPAA Risk and Security Committee. will determine if unsecured PHI was breached and make a recommendation to the HIPAA Covered Entity's Privacy Official as to potential harm to the individual whose PHI was involved. Kansas Health Information Network, Inc. will attempt to mitigate, to the extent practicable, any harmful effect resulting from the breach.
4. Kansas Health Information Network, Inc. is also responsible for notifying the applicable Covered Entity in a timely manner (as may be specifically defined in the Business Associate Agreement) of any resultant privacy or security breach that involves a patient or health plan member of the Covered Entity. Kansas Health Information Network, Inc. will provide any information readily available to assist the Covered Entity to follow federal and state laws to report such breach both to the affected individual and to the Secretary of the Department of Health and Human Services.

Procedure:

1. Kansas Health Information Network, Inc. workforce member notifies Kansas Health Information Network, Inc. President/Director of Privacy and Data Compliance (DPDC) of breach. See ***Security Incident Procedures: Response and Reporting.***
2. Kansas Health Information Network, Inc. HIPAA Risk and Security Committee is convened and works to stop the breach ASAP, including suspending access privileges to PHI as applicable.
3. Kansas Health Information Network, Inc. HIPAA Risk and Security Committee including legal expertise, reviews the executed Business Associate Agreement with the Covered Entity in question to ascertain if next steps are defined within the executed agreement. State laws may contradict or be more stringent than federal laws regarding breach notification. Legal counsel is responsible to provide respective state law identity theft and/or related breach specific information so that procedural steps contained in this policy reflect both state and federal requirements.

4. Kansas Health Information Network, Inc. President or Director of Privacy and Data Compliance (DPDC) contacts the Covered Entity Privacy Official to inform the CE of the potential issue and steps taken thus far to investigate and mitigate such report. NOTE: Breach investigation and notification procedures should have been discussed prior to project commencement and should be spelled out in Kansas Health Information Network, Inc. BAA.

    4.1. It is the responsibility of the CE to report the breach; however, either the BA or CE can investigate the breach and perform the risk analysis associated with the breach.

    4.2. A Covered Entity may choose to bypass the performance of the Risk Assessment and simply notify the individuals of an impermissible use or disclosure. Organization's should review and determine if this is their preferred business choice. As a matter of operation, it appears to the author's that at least some parts of the Risk Assessment would need to be conducted either way, in order to validate an impermissible use or disclosure. Therefore, this template is written considering that a Risk Assessment will always be performed.]

5. The Director of Privacy and Data Compliance (DPDC) and/or Legal Counsel will conduct an immediate review to investigate and validate if the information breached was unsecured PHI and to conduct a Risk Assessment to determine if data was compromised. This review will include the following actions:

    5.1. Document the nature and extent of the PHI involved including the types of identifiers and the likelihood of re-identification; [Consider expansion of the current Security Incident Reporting Form. Include specific details about the type of information (clinical, financial, demographic; paper, electronic or spoken). Be sure to list those elements considered inherently higher risk such as social security numbers; financial/credit card information; diagnosis of Mental Illness/Drug and Alcohol addiction; HIV; Family Planning, Genetic Testing. Include consideration of any types of data with enough variation to allow for someone to commit identity theft.]

    5.2. Document the unauthorized person who used the PHI or to whom the disclosure was made.

    5.3. Document whether the PHI actually was acquired or viewed.

    5.4. Document the extent to which the risk to the PHI has been mitigated.

    5.5. Document any other reasonable factors related to the incident.

    5.6. Document if the impermissible acquisition, access, use, or disclosure was of a "Limited Data Set" (LDS) that did not contain birth dates or ZIP codes. NOTE: An LDS not containing birth dates or ZIP codes has been deemed by the Secretary as an automatic "low probability."

    5.7. Determine (or work with CE DPDC/Legal Counsel to determine) if information breached was unsecured PHI in accordance with the DHHS Guidance document published in the Federal Register on April 27, 2009 which listed and described encryption and destruction as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

        5.7.1. If the PHI is considered unsecured, go to step "5.7.3." below.

        5.7.2. If the PHI breached was considered secure (in accordance with the above Guidance document and Kansas Health Information Network, Inc.'s use of technology), document such in the compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. This may include notifying legal counsel as appropriate.

            5.7.2.1. If after review, the PHI breached was considered ***unsecured***, take the following steps:

5.7.3. Assess (or work with CE DPDC/Legal Counsel to assess) whether or not the security or privacy of the PHI was "compromised". Compromised means that the breach of PHI/data poses a significant risk of financial, reputational, or other harm to the individual.

5.7.3.1. If the PHI breached is considered "compromised" go to step "5.7.3.3" below.

5.7.3.2. If the PHI breached is not considered "compromised" document such in Kansas Health Information Network, Inc.'s compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. This may include notifying legal counsel as appropriate.

5.7.3.3. If the PHI breached is considered "compromised", determine (or work with CE DPDC/Legal Counsel to determine) if such use or disclosure of PHI meets the breach exclusions.

5.7.3.4. Unintentional access to PHI in good faith in the course of performing one's job and such access does not result in further impermissible use or disclosure.

5.7.3.5. Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate or affiliated organized health care arrangement.

5.7.3.6. When PHI is improperly disclosed but the covered entity or business associate believes in good faith that the recipient of the unauthorized information would not be able to retain the information.

6. If the PHI considered compromised meets one of the exclusions listed above, document such in Kansas Health Information Network, Inc.'s compliance files and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. This may include notifying legal counsel as appropriate.
7. Document a final conclusion, based on the response of the above factors and whether or not the final probability that the PHI has been compromised is low, medium or high.
8. Based on the analysis and resulting findings performed above, the Privacy & Security Officer(s) and/or Legal Counsel will develop a plan to mitigate the harm, to the extent that this is practicable.
9. It is the responsibility of the Covered Entity to notify the individual and to report such issue to the Department of Health and Human Services Secretary. However, this may be delegated to the Business Associate. See *hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule.*
10. Using the breach notification log, list the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during such breach. This log enables a BA to document breach information that the Covered Entity is required to report to the Secretary of Health and Human Services.
11. The Privacy Security Officer will apply the Kansas Health Information Network, Inc. Sanctions for Violating Privacy and Security Policies and Procedures policy as appropriate.
12. The Director of Privacy and Data Compliance (DPDC) will prepare changes to policies and procedures, and/or provide necessary training, to reduce the likelihood of a similar breach in the future.
13. The allegation, risk assessment, mitigation plan/actions taken, results, record of disciplinary actions (if any), and supporting information will be documented by the President of Kansas Health Information Network, Inc., Director of Privacy and Data Compliance (DPDC). This material may be needed in the future to demonstrate Kansas Health Information Network, Inc.'s compliance.

14. The documentation will be retained by Kansas Health Information Network, Inc. in the Kansas Health Information Network, Inc. HIPAA Compliance file with a copy in the client's (CE) file for six years. When the contract with the CE terminates, all PHI belonging to the CE will be returned or destroyed upon termination of the contract, or at a later date if such action is not feasible at the time of the contract termination date and is agreed upon by both the CE and Kansas Health Information Network, Inc..

REFERENCE:45 CFR § 164.530(f)

See also: Sanctions for Violating Privacy and Security Policies and Procedures

Security Incident Procedures: Response and Reporting	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 007
Section: ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.400-414*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO), or assigned delegates
Policy:

Kansas Health Information Network, Inc. maintains a comprehensive internal privacy and security data protection and control program, which is coordinated by the Director of Privacy and Data Compliance (DPDC). Kansas Health Information Network, Inc. also maintains a base compliance program which functions to keep PHI protected and addresses issues of breach of security and privacy policies and procedures by monitoring and mitigating such issues. The internal privacy/security incident reporting process is the mechanism of both the security control and compliance programs, which allows for Kansas Health Information Network, Inc. to identify, investigate, respond, and resolve known and suspected privacy and security breaches and incidents. The policy, procedure, incident response program and statistics associated are reviewed on at least an annual basis. The actual reporting of incidents occurs in two ways:

1. Through the use of a Privacy/ Security Incident Reporting Form (Note: This is used for all of the Kansas Health Information Network, Inc. workforce members and may also be utilized by outside organizations/individuals such as contractors or business associates.)
2. As a result of monitoring pre-configured automated system security reports (Intrusion detection/information protection system (IDS/IPS) alerts), and use of internal audits and monitoring reviews to identify issues.

Regardless of mode of receipt, a chain of command process is used to first address and resolve the issue, report to the individual regarding breach notification and then communicate to all workforce members as a core component of training any necessary curriculum changes resulting from the incident(s). Workforce members are taught to use the reporting processes and reminded of the Free Exercise of Rights and/or offered to complete the report anonymously so that there is no fear of retribution for making such report.

Procedure:

1. All workforce members are trained to use the Privacy/Security Incident Reporting Form which can be completed anonymously, to report any suspicious privacy/security activities. Training includes mandatory incident response content for contractors and third parties. Specific occurrences which will trigger the completion of the form may include but not be limited to the following:
    1.1. Any suspicious or known breach of privacy/security by any workforce member for any reason known to be a violation or contradiction of Kansas Health Information Network, Inc.'s philosophy of protecting and safeguarding PHI. This includes issues originating by a known workforce member aka "insider threat".

1.2. Any suspicious or known breach of privacy/security/cyber security by an external third party for any reason known to be a violation or contradiction of Kansas Health Information Network, Inc.'s philosophy of protecting and safeguarding PHI.

1.3. Any suspicious activity uncovered as a result of a review of routine or random audit trail.

1.4. Request for audit log review of user activity (special authorization required).

1.5. Suspected or proven violation of protection of malicious software (introduction of malicious software).

1.6. Violation of Login Attempt (Using or attempting to guess another users' log in and/or password).

1.7. Sharing of passwords.

1.8. Inappropriate access to the internet.

1.9. Improper network activity.

1.10. Improper Email or Social Media Activity.

1.11. Inappropriate access by customer, client, patient/health plan member, contractor or business associate.

1.12. Suspicious documents (inconsistent identification information, photo or physical description, suspected altered or forged signatures).

1.13. Suspicious Medical Information (Patient/health plan member unaware of or denies information previously collected in the medical record, or other trigger that patient/health plan member information is inconsistent with that previously found).

1.14. Suspicious requests (mail returned even though attempts at verifying address have occurred), patterns of usage inconsistent with previous history, frequent ID card requests or replacement requests with change of address.

1.15. Personal Information Suspicious (known fraud associated with personal information, inability for person to authenticate via challenge/secret questions, personal information inconsistent with other information on file or that provided via external source, duplicate identifiers (SSN, Medicaid, Medicare cards).

2. Forms must be accurately and thoroughly completed within 24 hours of the incident (or sooner if the suspected or known breach causes serious risk to Kansas Health Information Network, Inc.) and forwarded immediately to the attention of the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC). In the event an organization or individual outside Kansas Health Information Network, Inc. provides the report, the same time frame and reporting procedure applies to the Kansas Health Information Network, Inc. workforce member in receipt of the report. The Form may be copied in duplicate in order to facilitate this process and should include at least the following information:

2.1. Date,

2.2. Name,

2.3. Title of submitter,

2.4. Reason for report,

2.5. Indication of whether or not the activity is suspected or known,

2.6. Indication of what application (s) or system(s) have been violated,

2.7. Identification of the user in question if appropriate, form may include a listing of the more common reasons for completing the report (listed above) and checkbox style.

2.8. A section of the form should include date received and notes for investigation, mitigation and further actions).

3. Upon receipt of completed Security Incident Report, or automated system security report, the Director of Privacy and Data Compliance (DPDC) will review (and conduct superficial investigation if necessary) in order to confirm the validity and level of risk associated with the reported incident in order place the report in priority with other reports for committee review.

4. The Kansas Health Information Network, Inc. HIPAA Risk and Security Committee. (see Designation of HIPAA Officials) will convene within a reasonable period of time (depending upon the level of risk of the incident) and as frequently as necessary to determine the following:

   4.1. Investigate and validate the facts included in the incident report, this should include assessment of possible damage to Kansas Health Information Network, Inc. and may include use of forensic investigation techniques.

   4.2. Determine if the incident needs to be reported to law enforcement, other authorities or the Computer Emergency Response Team (CERT) Coordination Center.

   4.3. Determine if unsecured protected health information was acquired or disclosed in a breach situation. If so, determine method to report to the Covered Entity (logbook or direct report) see DUTY TO REPORT SECURITY OR PRIVACY BREACH, NOTIFY AND MITIGATE THE EFFECT.

   4.4. Determine if the incident was a result of Insider Threat origin.

   4.5. Determine application of sanctions as necessary in accordance with the Sanctions Policy.

   4.6. Lessen or mitigate any harmful effects to the extent necessary and applicable including but not limited to managing reputation, public relations and leveraging lessons learned.

   4.7. Determine if issue should be evaluated as part of a larger review (such as part of ongoing risk analysis), and whether or not systems configuration and/or changes to other related Kansas Health Information Network, Inc. policies and procedures are necessary.

   4.8. Address communication and training to all affected workforce members if policies and procedures are to be implemented or modified in accordance with MAINTENANCE OF POLICIES AND PROCEDURES document.

5. All necessary actions, including outcomes, will be handled promptly and documented in accordance with Kansas Health Information Network, Inc. policy.

6. On a routine basis, but not less than annually, planned routine testing/exercises are conducted to assure the incident response capability is in place. Simulations are used and testing is inclusive of workforce members who are accountable for carrying out incidence response.

7. On a routine basis (quarterly) the Privacy/Security Officer should provide to Kansas Health Information Network, Inc.'s President aggregate reporting of all received privacy/security incident reports, and Kansas Health Information Network, Inc.'s response, including level of sanctions applied, mitigation attempts, and/or resulting changes to policies and procedures. This allows the information gained from the evaluation of security incidents to be used to identify recurring or high-impact issues and update the incident response and recovery strategy. Incidents should be factored into ongoing Risk Analysis and Risk Management processes and Contingency Planning exercises as well to assure vulnerability management revisions reflect Lessons Learned.

Complaints of Privacy or Security Practices	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 008
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.530(d)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

1. Complaints concerning Kansas Health Information Network, Inc.'s privacy or security practices will be directed to the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) who will investigate, respond and report such complaints to the CE.
2. When appropriate, changes will be made to Kansas Health Information Network, Inc.'s privacy or security practices and/or initiation of workforce retraining will occur.
3. Complaints that indicate a possible violation of Kansas Health Information Network, Inc.'s policies or applicable law will be referred to the President of Kansas Health Information Network, Inc. for possible action under Kansas Health Information Network, Inc.'s policies regarding employee discipline. See also ***Sanctions for Violating Privacy and Security Policies and Procedures***.
4. Complaints regarding privacy or security practices, and responses to these complaints, will be kept in the HIPAA file and in the electronic Complaint log for six years.
5. For those complaints that contain PHI of a CE, the complaint file will be returned or destroyed upon termination of the contract with the CE, or at a later date as agreed upon by Kansas Health Information Network, Inc. and the CE.

Procedures:

Kansas Health Information Network, Inc. workforce members will inform the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) of any privacy or security complaints immediately upon receipt of such complaint from a patient, health plan member, authorized personal representative, CE employee, vendor, BA of a CE, subcontractor or BA of Kansas Health Information Network, Inc. include, at a minimum:

- Name of the complainant;
- How the complainant can be reached (address, phone number);
- Date and time of the complaint;
- Name of the staff member who received the complaint;
- Nature of the complaint;

1. In addition to these reporting steps, the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) as soon as possible after receiving the complaint will document the fact that a complaint was made in the HIPAA Complaint Log. [Note: HIPAA does not require this.

Kansas Health Information Network, Inc. is implementing this step to demonstrate appropriate business practices and regulatory compliance.]

2. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will contact the individual making the complaint within one business day of receiving notice of the complaint. Contact will be made using the most efficient and immediate means available, preferably by telephone. The Director of Privacy and Data Compliance (DPDC) will document the date and time of their response on the HIPAA Complaint Log. If a voice mail is left, he/she will continue to pursue direct communication until it occurs.
3. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will request that the individual complete a written complaint form (if the original complaint was verbal or written in non-standard format). The form may be mailed to the individual after the initial conversation, it may be emailed to the individual (using encryption as appropriate), or if the individual is unable or unwilling to fill out the form, the Privacy & Security Officer can document the complaint as described by the complainant on the form.
4. The complaint will be reviewed with any individual(s) associated with Kansas Health Information Network, Inc. that have been identified in the complaint as well as with the President of Kansas Health Information Network, Inc.
5. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will notify the CE's Privacy & Security Officer if the complaint is regarding a patient or health plan member of the CE as soon as the investigation and determination has been completed.
6. All documentation regarding privacy and security complaints will be filed and maintained in the HIPAA file and the electronic complaint log for six years.
    6.1. For those complaints that contain PHI of a CE, the complaint file will be returned or destroyed upon termination of the contract with the CE, or at a later date as agreed upon by Kansas Health Information Network, Inc. and the CE.

When No Compliance Violation is Found- Steps to be completed by Kansas Health Information Network, Inc.'s Privacy & Security Officer

1. If a determination is made that there was no violation of Kansas Health Information Network, Inc.'s privacy or security policies, then document these findings on the complaint form.
2. Communicate with the individual and explain your findings; also provide the individual with a written record of the complaint resolution.
3. Document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.
4. If the individual is dissatisfied with the disposition of his or her complaint, refer this matter to:
    4.1 The Director of Privacy and Data Compliance (DPDC) of Kansas Health Information Network, Inc. and,
    4.2 The HIPAA Risk and Security Committee,
    4.3 The designated Privacy & Security Officer of the CE.
5. Document the outcome on the HIPAA Complaint Log. Include the following:
    5.1 Date that the complainant was notified of outcome.
    5.2 Outcome findings (Kansas Health Information Network, Inc. in violation or not in violation).
    5.3 Date that the CE was notified of outcome.
6. File and maintain all documentation of complaints in the HIPAA Compliance file and the electronic complaint log for six years.

6.1 For those complaints that contain PHI of a CE, the complaint file will be returned or destroyed upon termination of the contract with the CE, or at a later date as agreed upon by Kansas Health Information Network, Inc. and the CE.

Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) will complete the following steps when a Compliance Violation is found:

1. Discuss the complaint with the President of Kansas Health Information Network, Inc. as soon as possible to review the violation and develop a remediation plan.
2. If a determination is made that a violation of Kansas Health Information Network, Inc.'s privacy or security policies has occurred, document this fact on the complaint form.
3. Document the remediation steps on the complaint form and an action plan established to complete them.
4. Kansas Health Information Network, Inc.'s President will advise the appropriate workforce members or other persons (if any) who bear responsibility for privacy or security policy violations and impose the appropriate sanctions on responsible personnel.
5. Communicate with the individual and explain your findings; also provide the individual with a written record of the complaint resolution.
6. Document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the complaint form.
7. If the individual is dissatisfied with the disposition of his or her complaint, refer this matter to:
   7.1. The Director of Privacy and Data Compliance (DPDC) and.
   7.2. The President of Kansas Health Information Network, Inc., or if so directed.
   7.3. The designated Privacy & Security Officer of the CE.
8. Notify the Privacy Official and/or designated Privacy & Security Officer of the CE as soon as the investigation and determination has been completed. Provide the CE with the following information:
   8.1. Name of the complainant.
   8.2. How the complainant can be reached (address, phone number).
   8.3. Date when complaint received.
   8.4. Nature of the complaint.
   8.5. Description of complaint investigation and outcome.
   8.6. Description of remediation plan if determined necessary.
9. Report to the CE on a weekly or other pre-determined basis the status of the remediation plan until all corrective activities have been accomplished.
10. Document the outcome on the HIPAA Complaint Log. Include the following:
    10.1. Date that the complainant was notified of outcome.
    10.2. Outcome findings (Kansas Health Information Network, Inc. in violation or not in violation).
    10.3. Date that the CE was notified of outcome.
11. Develop or make any necessary changes to existing privacy or security policies, procedures, technical or other solutions that are required to address those complaints that are valid. Train all employees and independent contractors on any new or revised privacy or security practices.
12. File and maintain all documentation of complaints in the HIPAA Compliance file for six years.

Sanctions for Violating Privacy and Security Policies and Procedures	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 009
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.530(e)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

1. Members of the Kansas Health Information Network, Inc. *workforce* are subject to disciplinary action for violation of policies and procedures. Disciplinary action is utilized in order to hold workforce members accountable for their behavior as it relates to the use and disclosure of protected health information, including the application of the minimum necessary concept. Violations that jeopardize the privacy or security of PHI are particularly serious. This seriousness is reflected in the nature of the disciplinary action, up to and including termination of employment.

2. All workforce members are thoroughly trained on the consequences of violating privacy and security policies and the importance of cooperating with federal or state investigations or disciplinary proceedings. This training occurs upon initial employment and then on a routine and recurring basis in accordance with policy entitled TRAINING PROGRAM: USES AND DISCLOSURES IN SAFEGUARDING PHI. User Confidentiality Agreements or Acceptable Use Policies are reviewed and signed upon initial employment.
3. All members of the workforce will be treated fairly and equitably in the imposition of sanctions for privacy and security violations. All penalties for non-compliance resulting in sanctions will be applied consistently across Kansas Health Information Network, Inc.. Any and all breaches of privacy and security policies will result in immediate consequences in accordance with the defined penalties regardless of job status or reason for violation.
4. Sanctions will be integrated/referenced in Kansas Health Information Network, Inc.'s overall employee discipline policy. This policy will be in writing.
5. Management shall also reserve the right to monitor system and media device activity to ensure the enforcement of policies.
6. Sanctions applicable to *business associates* will be incorporated into business associate agreements.
7. Disciplinary actions due to breaches of privacy or security of PHI will be documented, and the documentation must be retained for six years. Disclosure of PHI in violation of policy is reportable under the ***Accounting of Disclosures of Protected Health Information*** policy.
8. No member of the workforce and no business associate will be subject to sanctions for a *disclosure* of PHI made in good faith in accordance with the following policies which function to assure Kansas Health Information Network, Inc. does not retaliate against an individual who performs whistleblower activity or reports PHI as a victim of a crime:

    8.1. Disclosure of Protected Health Information by "Whistleblowers".

    8.2. Disclosures of Protected Health Information by Workforce Members who are the Victims of a Crime.

Procedures:

1. All workforce members are trained to contact the Director of Privacy and Data Compliance (DPDC) in an expeditious manner whenever a suspected or actual violation of any Privacy and/or Security Policies and Procedures occurs. The violation may be reported in a variation of ways including but not limited to the following:
   1.1. Resulting from Management activity.
   1.2. Privacy Complaint.
   1.3. Security Incident Report.
2. Upon receipt of the report or notification, the Director of Privacy and Data Compliance (DPDC) will review the report in order to confirm the validity and level of risk associated with the reported violation.
3. The Director of Privacy and Data Compliance (DPDC) will consult any necessary workforce member, and/or Kansas Health Information Network, Inc. President as frequently as necessary to:
   3.1. Investigate and validate the facts included in the incident report. This should include assessment of possible damage to Kansas Health Information Network, Inc..
   3.2. Determine if legal counsel or other outside representation is necessary.
   3.3. Determine if mitigation is appropriate. Take into consideration if the individual attempted to mitigate the situation if applicable.
   3.4. Determine if other workforce members were involved or had knowledge of the violation and whether reasonable action should have been taken.
   3.5. Determine if report was conducted in bad faith or malicious in nature.
   3.6. Determine how to communicate and carry out disciplinary sanctions of any involved workforce members as necessary in accordance with the Sanctions Policy. This includes notifying defined personnel (e.g. Managers or Supervisors) within a defined time period (24 hours is suggested or as timely as possible) when a formal process is initiated for a subordinate. Additionally, if applicable, specific license, registration, and certification denial or revocations should be addressed.

Level of Breach	Example	Penalty
Improper and/or unintentional breaches	Workforce member unintentionally sends fax to restaurant as a result of careless keying of fax number.	Verbal warning for first offense. Increased workforce training on subject. Recurring violation warrants written warning with period of days to cure.
Unauthorized use or misuse	Workforce member uses Kansas Health Information Network, Inc. computer to download music and copy onto CD.	Written warning with clear direction that repeat offense will result in suspension and/or termination.
Willful and/or intentional disclosures	Workforce member searches for PHI in Kansas Health Information Network, Inc. system and sells it to public.	Termination of employment/contract. Other appropriate legal recourse.

4. All necessary actions, including outcomes, will be handled promptly and documented in accordance with Kansas Health Information Network, Inc. policy.
5. The President of Kansas Health Information Network, Inc. will document disciplinary actions in the employee's, subcontractor's or 2nd tier business associate's file, and will retain the documentation for at least six years.
    5.1. As required by federal (HIPAA) or state law and as stated in the BA contract with a CE, Kansas Health Information Network, Inc. will immediately report to the CE any accidental or unauthorized breaches of privacy or security of patient/health plan member's PHI.
    5.2. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will be responsible for contacting the Privacy Official of the applicable CE. This will be done as soon as the breach has been noted and reviewed by the President of Kansas Health Information Network, Inc..
    5.3. Kansas Health Information Network, Inc. shall use its best efforts to mitigate the deleterious effects of any use or disclosure of PHI not authorized by the BA contract.
    5.4. Kansas Health Information Network, Inc. will develop a written corrective action plan (CAP) describing the remedial actions taken or to be taken. This will be submitted to the CE within 30 days for approval.
    5.5. Workforce members of Kansas Health Information Network, Inc. will be trained on all remedial actions and changes in policies / procedures to prevent any future breaches.
    5.6. Once the breach has been reported by Kansas Health Information Network, Inc., the CE will determine whether the proposed corrective action plan presented by Kansas Health Information Network, Inc. is acceptable.
    5.7. The CE may accept or reject the CAP, require additional corrective action or terminate the relationship with Kansas Health Information Network, Inc..
    5.8. All breaches that are identified by, or reported to, Kansas Health Information Network, Inc. will be included in the accounting of disclosures for the applicable patient(s)/health plan member(s).
6. On a routine basis the Director of Privacy and Data Compliance (DPDC) will prepare aggregate reporting of all received privacy and security violation reports and the Business Associate's response, including level of sanctions applied, mitigation attempts and/or resulting changes to policies and procedures. The reports will be reviewed with the Kansas Health Information Network, Inc. President. The Director of Privacy and Data Compliance (DPDC) will periodically perform the following:
    6.1. Determine if each issue should be evaluated as part of a larger review (such as part of ongoing risk analysis) and whether or not computer systems configuration and/or changes to other related Kansas Health Information Network, Inc. policies and procedures are necessary in order to lessen the chance that similar workforce behavior/violation will reoccur.
    6.2. Address communication and training to all affected workforce members if policies and procedures are to be implemented or modified in accordance with the Maintenance of Policies and Procedures Policy.
7. Review Kansas Health Information Network, Inc.'s discipline policies to assure that breaches of security and privacy of PHI are dealt with adequately and fairly. Document disciplinary actions and retain the documentation for at least six years.

Email and Protected Health Information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 010
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.312(e) and 164.530(c)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

In general, protected health information (PHI) should not be transmitted by e-mail unless the sender is using a secure e-mail system. In accordance with Kansas Health Information Network, Inc. TECHNICAL SECURITY SAFEGUARDS, a secure e-mail system has the following features:

- *Transmission Security*. The message cannot be intercepted. If the message is sent over an open network (e.g. the Internet), it must be encrypted using an encryption standard approved by the Director of Privacy and Data Compliance (DPDC).
- *Mechanism to Authenticate*. The recipient of the message will know that the content has not been altered during transmission.
- *Person or Entity Authentication*. The recipient of the message will know the true identity of the sender.
- *Integrity Controls.* There are safeguards to lessen the possibility of sending the message to someone who is not authorized to receive it. There are safeguards to reduce the likelihood that the message will be forwarded to someone who is not an intended recipient. The email alerting process provides the Director of Privacy and Data Compliance with an alert to review outgoing emails potentially containing sensitive information. (KONZA Data Loss Prevention Policy.docx)
- *Encryption*. A mechanism to encrypt or transform confidential plaintext into cipher text in order to protect it. An encryption algorithm provides the process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Note: The only current way to protect your e-mail messages from interception is by encrypting the messages.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) and workforce supervisors will discuss Email communication of sensitive information including PHI, at the outset of new projects. Client preferences will be addressed in the Business Associate Agreement, documented internally on Client Information Management Checklist and communicated to project team members.
2. Unless otherwise informed by the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC), sensitive information will be sent in the following way:
   2.1. Users will send sensitive information via secure SFTP, encrypted email, or if encrypted email is not available, at the very least, sensitive information will be placed in a separate attached, password protected document.
      2.1.1. User will provide client with the password in separate email if needed.

Note: If used, this procedure is to be followed until a more robust solution is implemented by Kansas Health Information Network, Inc.

3. Refer to the following guidance for general email usage:

Workforce Accountability: Positive E-mail Usage Protocol

- Do use e-mail responsibly and productively to facilitate Kansas Health Information Network, Inc. business and maintain and enhance Kansas Health Information Network, Inc.'s image and reputation.
- Actively monitor and manage e-mail mailbox contents; periodically delete non-record messages no longer needed for reference; set the e-mail preference to automatically delete deleted message.
- Keep all distribution and e-mail addresses updated to avoid misdirection of information.
- Compress large files or documents using a tool like WinZip before attaching to an e-mail message; often a message exceeding 2 mega-bites will be returned as undeliverable.
- Keep a copy either in an e-mail mailbox folder, or a paper copy print out of any business record that originate through e-mail.
- Immediately report suspected phishing or interactions where others request sensitive and/or personal information.

Workforce Accountability: Email Use to Avoid/ A Message for the Workforce

- Do not use "Instant Message" programs as they are inherently not secure.
- Do not send any e-mail message that you would be embarrassed to find printed under your name on the front page of your local paper.
- Scrutinize email subject lines, sending and receiving information and be wary of potential phishing. Key potential triggers to indicate phishing might include but are not limited to misspellings, subject lines containing "too-good-to-be-true offers, addressing in a generic manner, use of links and attachment, demands to click, unreasonable free offers, bad grammar, threats and mass emails.
- When replying to an e-mail, do not include the prior message(s) in your response since the prior message(s) may contain PHI or other confidential information which either you or your recipient have copied or forwarded the information.
- Only use the reply-all feature when you are aware of the number and identity of the recipients.
- Avoid using graphics, clip art or other large images or backgrounds in your e-mail messages or e-mail signature; this will speed up delivery and save space in your e-mail mailbox.
- Personal use of e-mail should be limited and may not interfere with your work duties.
- Never use profanity in mail messages.
- Never access or distribute information that is obscene, abusive, libelous or defamatory.
- Do not distribute copyrighted material without written permission.
- Do not impersonate another user.
- Never access another's e-mail account without his/her permission.
- Do not send chain letters; these use vast system resources.
- Do not use all capital letters; this is like shouting in writing.

- Do not send e-mail messages to distribution lists unless you understand the purpose and the membership of the list.

4. The Director of Privacy and Data Compliance (DPDC) will assure all decisions related to the chosen solution(s) are documented and retained in accordance with the Kansas Health Information Network, Inc. retention policy. This includes documentation supporting "further assessment" activities ("Addressable" Implementation Specifications). If new processes and/or technical solution are chosen, the Privacy & Security Officer will assure the solution is implemented in a timely manner, any affected policies are updated and necessary training of such occurs as appropriate.
5. Routine monitoring of this solution will also occur in order to continually assess the effectiveness of Kansas Health Information Network, Inc.'s ability to balance the confidentiality of PHI with data integrity and availability.

Policies and Guidelines on Workstation Use and Security	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 011
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.310(b), (c) and 164.530(c)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

Kansas Health Information Network, Inc. will have secure work areas containing workstations with physical safeguards to minimize the possibility of unauthorized observation or access to *protected health information* (PHI). Areas where sensitive information is regularly entered or utilized will be secured using barriers to prevent public viewing of PHI. If the *worker* accessing the sensitive information must leave the workstation at any time, it will be his or her responsibility to remove the information being accessed from the workstation screen or to cover or file information being accessed in hard copy. Printers and fax machines, copy machines and shredders will be located in the most secure areas available and will not be located in or near areas frequented by *members* or the public. Kansas Health Information Network, Inc. will also provide appropriate security measures for portable workstations containing PHI.

Procedure:

The Director of Privacy and Data Compliance (DPDC) is responsible to choose the Kansas Health Information Network, Inc. preferred combination of technical solution and process to develop the procedures which function to reasonably safeguard protected health information and make up the workstation use and security. The following factors should be considered:

1. Reviewing the risk assessment results and related documentation.
2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
4. Thoroughly considering all areas defined below as “Implementation Considerations”.

Implementation Considerations for Workstation Use and Security

Workstation attendance: Protected health information can never be left unattended. Therefore, workforce with access to PHI must always lock or log out of their station before leaving it unattended. Workforce members must always lock away, turnover or otherwise make hard copies containing protected health information inaccessible to local foot traffic.

Control Methods:

1. Kansas Health Information Network, Inc. workstations and work areas that are used to access PHI are located in controlled areas that have physical protections including locks, key cards or similar devices.
2. Kansas Health Information Network, Inc. facility (facilities) is continuously monitored during business hours and security locked and alarmed at all other times.
3. Kansas Health Information Network, Inc. utilizes workstation inactivity timeouts and password-protected "screen savers." Other workstation locking mechanisms such as proximity-based locks, USB authentication devices and similar mechanisms may only be used with approval of Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC).
4. Kansas Health Information Network, Inc. takes steps to prevent unauthorized persons from casually viewing workstations or work areas located in public areas by locating monitors behind petitions or similar barrier and by installing blinds, covers or enclosures about monitors, using polarizing filters or other similar approved methods.
5. Kansas Health Information Network, Inc. positions the monitors away from outside windows, public hallways and customer areas.
6. Various versions of Microsoft Windows operating systems have varying degrees of security capability.

Portable Workstation Control: Due to the ease of theft, portable workstations require greater physical security controls. This may include physically attaching portable workstations with cable locks when left alone for long periods of time and/or the use of physical token devices or biometrics that will not allow the workstation to function properly without such access device.

1. The Director of Privacy and Data Compliance (DPDC) will assure that all decisions related to the chosen solution(s) are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This may include any risk and cost analyses undertaken to determine whether physical changes are needed to improve security of areas in which workstations are used. (Example analyses: costs of relocating equipment and wiring; installation of locking doors; and, purchase of shielding devices, security cable kits, portable token devices or other such security tools.) Additionally, such documentation includes "further assessment" activities in support of "Addressable" Implementation Specifications.
2. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will assure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process.
    2.1. This includes procedural development and implementation of chosen workstation use and control methods.
    2.2. Updating any and all related policies and procedures.
3. Training any and all affected workforce members based upon his/her job function.The Director of Privacy and Data Compliance (DPDC) will assure that routine monitoring of this solution is carried out routinely in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the PHI with its integrity and availability.
4. In order to emphasize the security of the physical environment and location considerations where electronic computing devices containing PHI are kept, the Director of Privacy and Data Compliance (DPDC) will periodically review the location and placement of all workstations, printers, facsimile machines, copy machines, shredders and all other areas where sensitive information is reviewed or processed. This may include inspecting content of data contained on workstations in order to determine if it is business related and appropriate.

Free Exercise of Privacy Rights	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 012
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.310(b), (c), 160.316 and 164.530(c)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

Kansas Health Information Network, Inc. representatives (when Kansas Health Information Network, Inc. is acting as a Business Associate of HIPAA Covered Entities) shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for the exercise by the individual of any right under, or for participation in, any process established by federal or state law or regulation, or Kansas Health Information Network, Inc. policies, including the filing of a complaint;
2. Any individual or other person for:
    2.1. Filing of a complaint with the Secretary of Health and Human Services in accordance with federal privacy regulations [45 CFR Part 160] or with the CE Notice of Privacy Practices, or any of its policies and procedures;
    2.2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C – Administrative Simplification, of Title XI of the Social Security Act; or
    2.3. Opposing any act or practice made unlawful by federal privacy regulations promulgated under the authority of Part C, Title XI of the Social Security Act, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of those regulations.
3. No member of the workforce of Kansas Health Information Network, Inc. shall require someone to waive the right to file a complaint with the Secretary of Health and Human Services, in accordance with federal privacy regulations [45 CFR Part 160], as a condition of the provision of treatment, payment, enrollment in a health plan, eligibility for benefits.

Procedures:

It is the responsibility of the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) to assure all Kansas Health Information Network, Inc. workforce members are trained on this policy.

Training Program: Uses, Disclosures, and Safeguarding Protected Health Information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 013
Section**:** ***One*** Subject: ***Workforce Policies***	Related Law(s): ***45 CFR § 164.530(b) and NPRM 45 CFR § 142.308(a)(12) and (b)(6)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

1. Kansas Health Information Network, Inc. understands that individual workforce members are a critical factor in protecting and securing PHI, confidential data, and systems. This protection level is improved/enhanced by education. Therefore, Kansas Health Information Network, Inc. has dedicated adequate time, resources, and tools for its workforce improvement/training program. All members of the Kansas Health Information Network, Inc. workforce, i.e., Kansas Health Information Network, Inc. employees and consultants, will receive training in the policies and procedures that apply to their jobs, including maintenance of the privacy and security of PHI. New members of the workforce will receive training as part of orientation to their jobs, and to Kansas Health Information Network, Inc., within a reasonable time of joining the workforce.
2. All workforce members will receive training in privacy and security prior to receiving access to PHI and no later than sixty days from hiring. Each workforce member will be trained on the products and services and security of the Kansas Health Information Network, Inc. This includes the Acceptable Use Agreement and expectations and acknowledgement of compliance with such by signing. The Acceptable Use Agreement defines system/data responsibilities and accountability as well as limits for use of the information and assets.
3. All members of the workforce will receive additional training as policies and procedures are changed, to the extent that the changes affect their jobs in addition to routine refresher training.
4. Attendance at training sessions and/or acknowledgement of review and understanding of privacy and security training will be documented to demonstrate that each member of the workforce has received training in accordance with this policy. The documentation must be retained for six years.
5. Agents or subcontractors hired by Kansas Health Information Network, Inc. to provide services requiring the use / disclosure of PHI on behalf of a CE (2nd Tier Business Associates) will also be required to receive privacy and security training as appropriate to their level of access to PHI.
6. Other individuals or organizations who are affiliated with Kansas Health Information Network, Inc. through either a contracted or an informal arrangement who may have indirect exposure to PHI of a CE will be required to sign a confidentiality agreement. This category would include any hardware or software vendors who are providing service to Kansas Health Information Network, Inc.; maintenance staff; temporary staff or volunteers.

Content of Training

Training sessions will include the following:

1. Awareness training: Threats to the privacy and security of protected health information and how Kansas Health Information Network, Inc. handles/stores PHI.
    1.1. How failure to protect against these threats can harm patients or health care members of a CE with whom Kansas Health Information Network, Inc. has been contracted.
    1.2. The importance of each member of the workforce maintaining compliance with privacy and security of PHI to minimize those threats and to report such compromises should they occur. Leading principles and practices for all types of information exchange of PHI including verbal, hard copy paper and electronic data are included.
    1.3. Notice of Privacy Practices (attached to this policy) may be used as a general Awareness training tool.
    1.4. Rules for user responsibility, acceptable behavior for email, use of internet, mobile device usage, teleworking, social media, facility usage and other information system usage are included. Cybersecurity responsibilities and Insider Threat awareness is included. Bring Your Own Device usage (if allowed) includes training on an approved list of applications, eligibility requirements, privacy expectations, data wipe, application stores, and application extensions and plugins.
    1.5. A separate and specific training program is in place for those workforce members playing a specified role in contingency planning and incident threat handling. See CONTINGENCY PLANNING.
2. Details of applicable policies and procedures:
    2.1. How privacy and security policies affect the job of each member of the workforce.
    2.2. How they define what is expected of each worker when they apply to services or activities performed by Kansas Health Information Network, Inc. as a BA with access to PHI.
3. Periodic reminders.
4. Timely information about changes in policies and procedures.
5. Workforce Systems Monitoring:
    5.1. Information is included that addresses how Kansas Health Information Network, Inc. will monitor workforce member actions and that management will take appropriate action when unauthorized activity occurs.
6. Information about sanctions:
    6.1. How members of the workforce may be sanctioned under Kansas Health Information Network, Inc. policy.
    6.2. Sanctions under state and/or federal law for breaches of privacy and security policies that may occur.
7. Testing: Kansas Health Information Network, Inc. may undertake testing to measure comprehension and retention of the material.

Procedure:

1. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will develop and maintain a privacy and security-training program for members of the workforce.
2. The program will include what members of the workforce need to perform their duties and access to PHI as necessary and appropriate. This training will be provided by Kansas Health Information Network, Inc.'s DPDC Director of Privacy and Data Compliance (DPDC) to workforce members in the Kansas Health Information Network, Inc. home office, and those members of the workforce who primarily work remotely, either at the client's location or from another office site including home office locations.
3. When determined to be in the client's best interest, any subcontractor, agent or other worker (2nd tier BA) employed by Kansas Health Information Network, Inc. on behalf of a CE will be treated as workforce and will be provided with privacy and security training in accordance with the access to PHI required to perform their duties. *[NOTE: Federal HIPAA privacy regulations do not explicitly require that business associates receive training.]*
4. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will include procedures in the training program to document the training given each workforce member in that worker's personnel record. Documentation of training of any agent or organization subcontracted by Kansas Health Information Network, Inc. will be filed with that individual or organization's contract. In lieu of training provided by Kansas Health Information Network, Inc., a signed BA-type agreement with the agent or organization will be required stating that they will be compliant with all applicable HIPAA privacy and security regulations.
5. The program will include follow-up procedures to assure that all members of the workforce have been included in the appropriate training. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will have the workforce member sign and date that he/she has received, reviewed and will agree to implement the training materials that have been provided. This includes but is not limited to training the following types of workers; senior executives, business unit security Points of Contacts and System/Software Developers in their specific roles/responsibilities related to safeguarding PHI.
6. The Director of Privacy and Data Compliance (DPDC) will develop new training materials whenever a material change in policies and procedures occurs so that changes may be incorporated. This includes confirming that plans for security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency and alignment with the risk management strategy and response priorities.
7. All affected members of the workforce, and if applicable, subcontracted individuals or organizations (2nd tier BAs) will be trained by Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) in material changes to policies and procedures related to privacy and security of PHI prior to the effective date of the change. If this is not possible, the training will take place within a reasonable period of time after the change takes effect. Training in changed policies and procedures will be documented by Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC).
8. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) is responsible to conduct a routine review of the effectiveness of the privacy and security training program and to assure risk assessment results are coordinated and integrated into the program on an ongoing basis.
9. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will be responsible for filing all training materials and curriculum that will be retained in the HIPAA Compliance files in the home office for six years after the date they are superseded by revised materials.

10. Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will document training for each member of the workforce who receives training in accordance with this policy and will assure that this documentation be retained for each workforce member in the home office, for six years. *[NOTE: Federal HIPAA privacy regulations require documentation of training. Kansas Health Information Network, Inc.'s President will determine what constitutes acceptable documentation (e.g. sign in sheets, class attendance lists maintained by instructor, log-in record for electronic training materials, etc.)]*

SECTION TWO – PRIVACY & SECURITY POLICIES

Determination of Relationship Between Covered Entities & Kansas Health Information Network, Inc.	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 014
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.502(e) and 164.504(e); 67 FR53264-53266*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC)

Policy:

1. Per the HIPAA Rule, no member of a CE's workforce is permitted to disclose protected health information (PHI) to a business associate (BA), i.e. Kansas Health Information Network, Inc., or to allow Kansas Health Information Network, Inc. to obtain PHI on behalf of the CE, unless a written agreement (business associate agreement – BAA) has been executed between the CE and Kansas Health Information Network, Inc.. This agreement must include provisions that meet the standards listed in this agreement.
2. No member of a CE's workforce is permitted to disclose protected health information (PHI) to Kansas Health Information Network, Inc.'s workforce (employees and subcontractors) and Kansas Health Information Network, Inc.'s workforce is not permitted to seek PHI unless Kansas Health Information Network, Inc. requires the information in order for it to perform the services for which the CE has contracted with it.
3. Kansas Health Information Network, Inc. is not permitted to disclose protected health information to another business associate of the CE unless a written agreement has been executed between KHIN, the CE and that business associate.
4. If the CE learns that Kansas Health Information Network, Inc. has materially violated its BA agreement, the CE will notify Kansas Health Information Network, Inc. Kansas Health Information Network, Inc.'s failure to cure the breach within a reasonable time period will likely result in termination of the agreement.
5. Kansas Health Information Network, Inc. may encounter PHI, in the process of performing its duties under its project contracts, and since the CE has a duty to safeguard PHI, all the Kansas Health Information Network, Inc. agreements for non-exchange type services will contain the basic confidentiality clause identified later in this policy.
6. Kansas Health Information Network, Inc. and the CE will be required to execute a business associate agreement when Kansas Health Information Network, Inc. will perform one of the following types of services to or on behalf of the CE when the specific role requires use of PHI. Other projects may also require a BAA if Kansas Health Information Network, Inc. will require access to PHI to complete its contracted obligations.

   Types of Relationships that Typically Require a Business Associate Agreement Between a Covered Entity and Kansas Health Information Network, Inc.

   6.1. Health care clearinghouse (an organization which transmits electronic transactions to, or receives electronic transactions from, other organizations on behalf of the CE).

   6.2. Fundraising or marketing.

   6.3. Mailing.

6.4. Data analysis or data aggregation of any kind, including services that de-identify PHI.

6.5. Professional services, such as consulting, legal, accounting and auditing, actuarial, management or administration, financial, etc.

6.6. Accreditation.

6.7. Electronic data processing, including software and hardware maintenance.

6.8. Photocopying claims and other sources of PHI.

6.9. Document shredding.

6.10. Repricing (such as performed by a preferred provider organization to apply negotiated discounts to claims).

6.11. Storage of PHI (both paper records and electronic media).

6.12. Outsourced services, such as billing or collections, that involve PHI in any way.

6.13. Web site hosting.

6.14. Collection of PHI from patients or health plan members of the CE.

6.15. Board members may be considered workforce members or business associates depending on the nature of the association to the CE and the nature of the services / activities performed by the Board.

7. If a BA is required by law to perform a function or activity on behalf of the CE, or to provide a service described in the definition of "business associate" (See ***Definitions***), the CE may disclose protected health information to Kansas Health Information Network, Inc. to the extent necessary to comply with the legal mandate. Kansas Health Information Network, Inc. and the CE will attempt in good faith to reach an agreement that meets the standards of this policy, and, if such attempt fails, will document the attempt and the reasons that the agreement cannot be obtained.

Standards for Business Associate Agreement

8. All contracts between the CE and Kansas Health Information Network, Inc. must contain the following statements or provisions:

8.1. A description of the services to be performed by Kansas Health Information Network, Inc. for, or on behalf of, the CE including a description of the uses and disclosures of the CE's PHI permitted to and required of Kansas Health Information Network, Inc..

8.2. A statement that Kansas Health Information Network, Inc. will not use or further disclose the CE's PHI other than as permitted by HIPAA or required by the contract or as required by law, and will not use or disclose PHI in a manner that would violate the requirements of the CE's policies and procedures, and applicable law, if done by the CE.

8.3. A statement that Kansas Health Information Network, Inc. will use appropriate safeguards to prevent use or disclosure of the CE's PHI other than as provided for by its contract.

8.4. A statement that Kansas Health Information Network, Inc. will report to the CE as soon as possible any use or disclosure of the CE's PHI not provided for by its contract, of which it becomes aware.

8.5. A statement that Kansas Health Information Network, Inc. will require any agent or a subcontractor, to whom the Kansas Health Information Network, Inc. (as the BA) provides the CE's PHI, to agree in writing to the same restrictions and conditions that apply to the BA with respect to such PHI.

8.6. A statement that Kansas Health Information Network, Inc. will make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the CE available to the Secretary of the

federal Department of Health and Human Services for purposes of determining the CE's compliance with federal regulations concerning the privacy of PHI.

8.7. If feasible, within 30 days of the termination of the contract, Kansas Health Information Network, Inc. will return or destroy all of the CE's PHI that it still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information impractical.

8.8. The CE may terminate the agreement at any time if it determines that Kansas Health Information Network, Inc. has violated a material term of the agreement, and fails to cure such breach within 30 days of being so notified by the CE. If termination due to failure to timely cure a material breach is unfeasible for some reason, the CE is required to inform the Secretary, Department of Health and Human Services, of this fact.

8.9. A statement that Kansas Health Information Network, Inc. will be expected to implement adequate safeguards for PHI that will be exchanged or transmitted between Kansas Health Information Network, Inc. and the CE, and delineates the means to be employed by each party for safeguarding the integrity and confidentiality of the data exchanged.

8.10. A statement that Kansas Health Information Network, Inc. will within 30 days of receiving a prior written request, make available during normal business hours at its offices, all records, books, agreements, policies and procedures relating to the use or disclosure of the CE's PHI for purposes of enabling the CE to determine Kansas Health Information Network, Inc.'s compliance with the terms of their agreement.

8.11. A statement that Kansas Health Information Network, Inc. will immediately discontinue use or disclosure of the CE's PHI pertaining to any individual when so requested by the CE or the individual. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

8.12. A statement that Kansas Health Information Network, Inc. will accept from the CE such amendments to their business associate agreement as may subsequently be necessary to comply with changes in federal or state law regarding the security or privacy of PHI, or that Kansas Health Information Network, Inc. may terminate the agreement without prejudice if it is unable to comply with any such amendment.

9. Contracts between the CE and Kansas Health Information Network, Inc. may contain the following statements or provisions, as may be applicable to the circumstances of their BAA.

9.1. A statement that Kansas Health Information Network, Inc. is permitted to use protected health information for its own proper management and administration, or to carry out its legal responsibilities.

9.2. A statement that Kansas Health Information Network, Inc. may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that:

9.2.1. The disclosure is required by law, or.

9.2.2. That Kansas Health Information Network, Inc. has obtained from the third party:

- Reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by Kansas Health Information Network, Inc.; and
- An agreement to notify Kansas Health Information Network, Inc. of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached.

10. The contract may permit Kansas Health Information Network, Inc. to provide data aggregation services relating to the CE's health care operations. Data aggregation means the combining of the CE's protected health information with the protected health information of other organizations, to permit data analyses that relate to the health care operations of the respective organizations.
11. If the contract calls for Kansas Health Information Network, Inc. to de-identify the CE's PHI, it must contain a requirement to comply with HIPAA. The contract shall also contain a statement that de-identified health information does not constitute PHI as defined in the business associate agreement with the CE.
12. If the contract calls for Kansas Health Information Network, Inc. to create a limited data set from the CE's PHI, it must contain a requirement to comply with the HIPAA's "Limited Data Set" policy, and to provide the CE with documentation of compliance with this policy. The contract shall also contain a statement that information in a limited data set health information constitutes PHI as defined in the business associate agreement. [NOTE: If Kansas Health Information Network, Inc. will also use the limited data set it creates, it must execute a data use agreement with the CE. See the Secondary Data Use Policy and ***Limited Data Set*** Policy.]

Attached to this policy are business associate contract provisions suggested by the Federal Department of Health and Human Services, as published in the Federal Register, 67 FR 53264 – 53266 and Kansas Health Information Network, Inc.'s sample Business Associate Agreement.

Basic Confidentiality Clause

The following clause may be included in contracts between Kansas Health Information Network, Inc. and a covered entity doing business with Kansas Health Information Network, Inc. when the relationship is not as a business associate, however, in the course of performing contractual responsibilities, Kansas Health Information Network, Inc. staff and/or subcontractors may inadvertently come into contact with protected health information.

[NOTE: The following is provided only as an example.]

> "Protected health information (abbreviated PHI) means information, including demographic information, whether oral or recorded in any form or medium, that relates to an individual's health, health care services, or payment for services and which identifies the individual. (This includes information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and includes information that could reasonably be used to identify the individual, such as social security number or driver's license number, even if the name is not included). Kansas Health Information Network, Inc. hereby represents and warrants that its employees, subcontractors, and others performing duties under this contract, have been instructed to maintain the confidentiality of PHI of which they may become aware in the course of their duties under this contract. Kansas Health Information Network, Inc. will assure that appropriate supervision and disciplinary measures are in place to minimize the incidental exposure to or disclosure of PHI. Kansas Health Information Network, Inc. will report to the CE any instances of which it becomes aware in which PHI is improperly stored or disclosed, whether by employees or subcontractors of Kansas Health Information Network, Inc., employees of the CE, or other persons."

Procedure:

1. For projects beyond the standard health information exchange services provided by KHIN, a CE's representative and the Kansas Health Information Network, Inc. President will review the proposed Project Description to determine if the Kansas Health Information Network, Inc. project creates a business associate requirement between the CE and Kansas Health Information Network, Inc. If a Business Associate relationship exists, the CE's Privacy Official or other corporate representative will:

    1.1. Meet with the CE representative (in person or via phone) and review the Information Management Checklist.

    1.2. Either draft a proposed Business Associate Agreement (BAA) or use the Kansas Health Information Network, Inc. BAA as their Agreement for the project (see sample Kansas Health Information Network, Inc. BAA attached to this policy).

2. The Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) will confer with the Kansas Health Information Network, Inc. President and if necessary, with the CE's employee who has responsibility for each business associate contract, to determine what provisions need to be added to the contract to comply with this policy and with applicable state and federal law regarding the privacy and security of PHI.

3. Any proposed BAA contract which involves giving Kansas Health Information Network, Inc. access to PHI, must be referred to the Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) or the Kansas Health Information Network, Inc. President for review prior to execution or renewal, to assure compliance with this policy. The Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) will include the Kansas Health Information Network, Inc.'s President or others in this review, as necessary.

4. The President of Kansas Health Information Network, Inc. and or Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will confer, with a member of the CE's workforce who is primarily responsible for each business associate relationship, to establish procedures to report material breaches of the business associate agreement.

    4.1. Material breaches discovered by Kansas Health Information Network, Inc. workforce or subcontractors are required to be reported to Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) and to the Kansas Health Information Network, Inc. President.

        4.1.1. The Director of Privacy and Data Compliance (DPDC) of Kansas Health Information Network, Inc. will notify the CE's Privacy Official of such material breaches.

        4.1.2. Kansas Health Information Network, Inc. will make all attempts to cure such breach within the 30- day period.

    4.2. When a material breach is found by or reported by another party to the CE, the CE's Privacy Official will so inform Kansas Health Information Network, Inc..

        4.2.1. Kansas Health Information Network, Inc. will make all attempts to cure such breach within the 30- day period.

        4.2.2. If Kansas Health Information Network, Inc. fails to cure the breach to the satisfaction of the CE within 30 days, the CE may send notice of immediate termination of the agreement or,

    4.3. If in consultation with the member of the CE's workforce who is primarily responsible for the business associate relationship, determines that the agreement cannot feasibly be terminated in spite of failure to cure the breach, the CE's Privacy Official or CE's General Counsel will so notify the Secretary of the Federal Department of Health and Human Services (DHHS).

5. All findings and correspondence regarding a material breach of a business associate agreement will be retained for six years following the date such contract is terminated, or, if termination is not feasible, documentation must be retained for six years from the date that notice is sent to the Secretary, DHHS.

Documentation will include a description of the reason or reasons why it is not feasible to terminate the contract.

6. All business associate contracts will be retained in the Kansas Health Information Network, Inc. Client files for a period of at least six years after the date when they are no longer in effect.

Cooperation with Federal Complaint Investigations and Compliance Reviews	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 015
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 160.300-314*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC)

Policy:

Kansas Health Information Network, Inc. will cooperate with duly authorized representatives of the federal Department of Health and Human Services (DHHS) in their investigation of complaints filed under federal regulations regarding the privacy of *protected health information* (PHI), and with their review of operations to determine whether Kansas Health Information Network, Inc. complies with federal regulations regarding the privacy of protected health information.

Cooperation includes providing access, during normal business hours, to policies, procedures, practices, facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to the complaint investigation or compliance review. Access will be provided at times other than normal business hours, and without prior notice, when the DHHS determines that circumstances require such access. DHHS access to protected health information is not limited by "*minimum necessary*" provisions of federal regulations pertaining to the privacy of protected health information ["HIPAA privacy regulations," 45 CFR § 164.502(b)], or by Kansas Health Information Network, Inc.'s MINIMUM NECESSARY RULE.

Kansas Health Information Network, Inc. will also maintain records and submit reports as the DHHS determines necessary to ascertain whether Kansas Health Information Network, Inc. is in compliance with federal regulations regarding the privacy of protected health information. These records and reports will be maintained and submitted in compliance with time, manner, and content requirements as prescribed by the DHHS.

Any DHHS investigation, and any disclosures of PHI by Kansas Health Information Network, Inc. in connection with such an investigation, must be in accordance with applicable laws and regulations, and specifically in accordance with the provisions of 45 CFR § 160.306, 160.308, 160.310, and 160.312.
Procedure:

A. Request for access to facilities or records.

1. Any employee who receives a communication from the DHHS, that requests access to any record, document or other information, will immediately notify the Privacy and Security Officer. This applies to requests received in writing, by telephone, or in person.
2. The Privacy and Security Officer will notify the Chief Executive Officer that a DHHS investigation or compliance review has been initiated.
3. The Privacy and Security Officer will determine whether the request complies with the applicable regulations, specifically 45 CFR § 160.306, 160.308, and 160.310.

4. If the Privacy and Security Officer determines that the request for access DOES NOT comply with the regulations, access will not be granted. The Privacy and Security Officer will communicate directly with the representative from DHHS, explaining the reason for not granting access, and will pursue such legal action as is necessary to protect Kansas Health Information Network, Inc.'s PHI from unwarranted *disclosure* in violation of federal regulations.
5. If the Privacy and Security Officer determines that the request DOES comply with the regulations, authorized representatives of DHHS will be granted access to Kansas Health Information Network, Inc.'s facilities and records, as necessary, to conduct the investigation or review.
6. The Privacy and Security Officer will designate an official to respond to DHHS requests for access. This must include designation of an official who will respond in the event of a request for immediate and unannounced access. The Privacy and Security Officer will also designate an alternate so that an official is always available to respond promptly to a DHHS request for access.
7. The official appointed by the Privacy and Security Officer will require DHHS representatives to present identification, and satisfactory evidence of their authority to receive access, prior to granting them access to any protected health information.
8. DHHS representatives who are conducting an investigation or review will be accommodated in a designated document room.
9. An individual assigned by the Privacy and Security Officer shall be located in the vicinity of the designated document room at all times when the DHHS representatives are present, to assist the representatives with document requests, to log all documents delivered to the document room, to log all copies made for the DHHS representatives, and to log the DHHS representatives' arrival and departure times.
10. The DHHS representatives will be required to request records and other documents in writing.
11. Requests for copies of documents to be removed from Kansas Health Information Network, Inc. premises must be in writing, and an individual designated by the Privacy and Security Officer will record all such copies in a log.
12. DHHS representatives will be escorted by an official designated by the Privacy and Security Officer at any time they require access to another part of Kansas Health Information Network, Inc. facilities, other than the designated document room.
13. The Privacy and Security Officer will assure that the CEO is kept apprised of the status of the investigation, or of the status of the DHHS request in the event access has been denied.

B. Request to keep records or submit reports

1. In the event that any Kansas Health Information Network, Inc. employee receives a request from DHHS to maintain records or submit reports to enable DHHS to determine whether Kansas Health Information Network, Inc. is complying with federal regulations regarding the privacy of protected health information, the request will be referred immediately to the Privacy and Security Officer, the Director of Medical Records, and the Director of Information Systems.
2. The Privacy and Security Officer, the Director of Medical Records, and the Director of Information Systems will discuss the request to determine whether it complies with applicable regulations, and whether it is feasible to comply. They will also estimate the cost of compliance.
3. Based on this review, the Privacy and Security Officer will either agree to maintain the requested records or submit the requested reports or will appeal the request to DHHS on the grounds that the request is either (a) not in compliance with applicable regulations, (b) not feasible, or (c) unreasonably costly.

4. The Director of Information Systems will assign responsibility for maintaining the records or preparing the reports, including responsibility for assuring that reporting time requirements are met.

C. Response to a finding of non-compliance

If DHHS issues a finding of non-compliance either verbally or in writing, following an investigation or compliance review, the Privacy and Security Officer will review the finding and decide how to reply. In accordance with regulations, the Privacy and Security Officer will contact DHHS representatives to attempt to resolve the matter by informal means. Any proposed resolution will be presented to the CEO for final approval.

In the event that the matter cannot be resolved informally, the Office of Privacy and Security Officer will contact counsel to prepare to defend Kansas Health Information Network, Inc.'s position.

D. Record keeping

The Privacy and Security Officer will keep detailed records in connection with a DHHS investigation or review. This includes records of all communications with DHHS representatives, all internal communications regarding the matter, all logs, analyses, and other documents prepared, and all findings presented by DHHS. Such records will be maintained for at least six years after the investigation has been closed. [NOTE: Federal HIPAA privacy regulations do not require that this documentation be retained. However, it is recommended in order to demonstrate compliance.]

REFERENCE: 45 CFR § 160.306, 160.308, 160.310, and 160.312

See Also: MINIMUM NECESSARY RULE

Verification of the Identity and Authority of a Person Requesting Disclosure of PHI	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 016
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.514(h)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

The Director of Privacy and Data Compliance (DPDC) of Kansas Health Information Network, Inc. shall take reasonable steps to authorize the disclosure of PHI:

1. Verify the identity of the person to whom the PHI is disclosed, and
2. Verify the person's authority to receive the PHI.

Disclosure of PHI

1. KANSAS HEALTH INFORMATION NETWORK, INC. provides a Personal Health Record (PHR) including all information that has been contributed into KANSAS HEALTH INFORMATION NETWORK, INC. National Network.
2. PHR accounts are only given to individuals greater than or equal to 18.
3. PHI may be disclosed to an individual who is involved in the patient's or health plan member's care, payment for such care, or to a personal representative, once the person's identity or relationship to the patient or health plan member has been verified. Such requests will first be referred by Kansas Health Information Network, Inc. workforce to Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) (or to the CE's Privacy Official if Kansas Health Information Network, Inc.'s workforce member is onsite) to determine whether or not to allow the disclosure.
4. All applicable Kansas Health Information Network, Inc. policies must be followed whenever PHI is disclosed to public officials without the patient's or health plan member's authorization of the applicable CE.

Verification of Identify

5. The KANSAS HEALTH INFORMATION NETWORK, INC. Help Desk provides identity proofing through verification of patient's medical information as part of the account provisioning.
   - 5.1. Providers listed on the care record.
   - 5.2. Address and telephone number.
   - 5.3. Facilities where care was received.
6. If a worker or subcontractor of Kansas Health Information Network, Inc. knows the identity and authority of the recipient of the PHI, and that person is an employee of the CE who has a known purpose for the PHI, no further documentation is necessary.

Procedures:

Before approving disclosures of PHI to entities other than the CE, all Kansas Health Information Network, Inc. workers or subcontractors will contact Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC).

1. For all requests for disclosure, the following information will be recorded by the Kansas Health Information Network, Inc. person who has been requested to make the disclosure, or by the Director of Privacy and Data Compliance (DPDC) on that person's behalf:
    1.1. Identity of patient or health plan member.
    1.2. Date of disclosure.
    1.3. Description of information disclosed.
    1.4. Reason for disclosure.
    1.5. Identity of the person (and contact information) to whom the disclosure is made.
    1.6. How the identity and authority of the recipient were verified.
2. All disclosures that are accountable disclosures will be recorded in the "PHI Disclosure Requests & Disclosures Accounting" log and maintained for six years.

Disclosure of PHI to Personal Representatives	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 017
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.502(g),(1),(2),(3),and (5)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

In applying Kansas Health Information Network, Inc.'s policies and procedures relating to the use or disclosure of protected health information when Kansas Health Information Network, Inc. is contracted as a business associate of a covered entity, a personal representative will be treated the same as the individual to whom the PHI pertains. This includes the right to examine and receive a copy of the individual's protected health information (PHI), to request an accounting for disclosures of PHI.

This policy gives personal representatives the same broad rights of access as applied to the patient or health plan member himself or herself. It is limited to people who are legally authorized to act on behalf of the patient or member of a covered entity.

Exceptions:

1. Kansas Health Information Network, Inc. does not disclose PHI to minors. Minors are defined as individuals under the age of 18.
2. Kansas Health Information Network, Inc. encourages the requestor to contact the facility that created the minor's medical record.

Accounting of Disclosures for Protected Health Information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 018
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.528*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy: The Kansas Health Information Network is not a Covered Entity and it does not create any health information. The Kansas Health Information Network aggregates information and is not the original source of any health information. Thus, requests to KHIN for a disclosure of health information will be sent to the Covered Entity that created it. In all instances requests will be forwarded to the CE that created the health information.

If a disclosure is requested for the aggregate record maintained by KHIN, then KHIN will provide the following information.

1. Disclosures of protected health information that are required by law – general policy.
2. Disclosure of protected health information for public health purposes.
3. Disclosure of protected health information to report child abuse, or other abuse, neglect, or domestic violence.
4. Reporting protected health information to employers under OSHA and similar laws.
5. Disclosure of protected health information to regulators.
6. Subpoenas, court orders, discovery requests, other legal processes that require the disclosure of protected health information.
7. Disclosure of protected health information for law enforcement purposes.
8. Use and disclosure of protected health information for purposes of research.
9. Disclosure of protected health information without authorization, to avert a serious threat to health or safety.
10. Disclosure of protected health information for certain government functions (includes PHI of members of the military, disclosures related to protective services of the president and others, but excludes national security or intelligence purposes, as noted under "exceptions," below.)
11. Disclosure of protected health information to workers' compensation programs.
12. Extension of privacy protection to deceased individuals.
13. Disclosure of protected health information by "whistleblowers".
14. Disclosures of protected health information by workforce members who are the victims of a crime.

Those disclosures that are to be tracked in an accounting are everything ***except*:

1. Disclosures made to carry out treatment, payment or health care operations.
2. Disclosures made to individuals (patients or health plan members).

3. Disclosures made for a facility's directory.
4. Disclosures made to persons involved in the individual's care.
5. Disclosures to authorized federal officials for purposes of national security or intelligence purposes.
6. Disclosures regarding prisoners made to correctional institutions or law enforcement officials.
7. Disclosures that occurred prior to the compliance date for Kansas Health Information Network, Inc. (April 14, 2003).
8. Disclosures of PHI to personal representatives.
9. Disclosures of PHI to disaster relief agencies.
10. Disclosures incidental to those allowed by Kansas Health Information Network, Inc. or applicable federal or state law.
11. Disclosure of information in a limited data set.
12. Disclosures that occurred more than 6 years prior to the date of the request for the accounting, or outside the time period to which the request applies.
    - The accounting must include any other disclosure that is made without the member's written authorization, unless the disclosure falls within one of the exceptions listed above (#2). This includes any disclosure made in violation of Kansas Health Information Network, Inc. policy, or federal or state law, regarding the privacy, security or confidentiality of PHI.
    - The accounting must include disclosures made by employees or subcontractors of Kansas Health Information Network, Inc. for any of the reasons listed above in #1 and # 3.

Procedures:

1. Any employee or subcontractor of Kansas Health Information Network, Inc. shall forward all requests for disclosure accounting received from to Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC). All requests should be provided in writing with the following information:
    1.1. Name and other identification of individual for whom accounting of disclosures was requested.
    1.2. Date when request was made.
    1.3. To whom and where health information is to be forwarded.
    1.4. Dates liable for accounting of disclosure.
2. If an individual who is a "covered individual" of the CE (patient, member of health plan, personal representative of a patient or of a health plan member) contacts Kansas Health Information Network, Inc. directly, the "covered individual" will be instructed to contact the CE instead to make the request Contact information will be provided to the "covered individual".
3. The Kansas Health Information Network, Inc. employee or subcontractor who receives a request from a "covered individual" or other person will obtain the following information:
    3.1. Name of the requestor and relationship to individual for whom disclosure accounting is being requested.
    3.2. Address and phone number(s) where individual can be reached.
    3.3. Contact date by the requestor.
    3.4. The Kansas Health Information Network, Inc. employee or subcontractor will notify (within one business day) Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) when this has occurred.

3.5. The Director of Privacy and Data Compliance (DPDC) will document the above information.

4. When a written request from the CE for a disclosure accounting to a "covered individual" of the CE is received, the Director of Privacy and Data Compliance (DPDC) will review the request to ensure the necessary information has been provided by the CE. This review will verify that the request is for health information disclosures that are required by HIPAA **AND** are for health information that has been, received, transmitted or maintained by Kansas Health Information Network, Inc..

5. The Director of Privacy and Data Compliance (DPDC) will review the records and compile a list of every disclosure for the past six years that is subject to an accounting. This review is to ensure that each entry contains:

   5.1. If available, the name and contact information of the individual for whom the disclosure accounting was provided.

   5.2. The name, address of the designee and the respective organization (CE) that received the information.

   5.3. Date that Kansas Health Information Network, Inc. provided the disclosure information to the CE or to the individual.

   5.4. A description of the information disclosed.

   5.5. A statement of the purpose of the PHI disclosure (if available a copy of the signed authorization or the request for disclosure).

   5.6. Any relevant documentation, such as a written request from a government or law enforcement agency.

6. If the request received by the CE is from a regulatory or law enforcement agency, the Director of Privacy and Data Compliance (DPDC) will review the request with the CE's Privacy Official. [Note: If it is a written statement that the agency provided the CE indicating that notification to the patient about a disclosure to that agency would be likely to impede that agency's activities, then the statement must specify the time period during which the patient is not to be informed of the disclosure. If the agency cannot immediately provide a written statement, an oral statement is acceptable but for a period of no more than 30 days. The oral statement, identity of the agency and official must be documented. In these two situations, the disclosure information will be omitted from the disclosure accounting.]

7. If many disclosures were made to the same entity for the same purpose, it is permissible to group them together by providing the following:

   7.1. The information provided in step 4 above.

   7.2. How frequently or how many times the information was disclosed.

   7.3. The date of the last such disclosure.

8. If there were no disclosures made by Kansas Health Information Network, Inc. for the individual requesting the accounting of disclosures, the Director of Privacy and Data Compliance (DPDC) will contact the appropriate designee of the CE with this information and document this.

9. The Director of Privacy and Data Compliance (DPDC) will be responsible for documenting the request and the information provided in the disclosure accounting (or notification of no disclosures) provided to the CE. He/she will also assure that this documentation be placed in Kansas Health Information Network, Inc.'s HIPAA compliance file in hard copy and in an electronic log for a period of six years, unless the contract with the CE terminates prior to the 6-year retention period.

10. When the contract with the CE terminates, all PHI belonging to the CE will be returned or destroyed upon termination of the contract, or at a later date if such action is not feasible at the time of the

contract termination date and as agreed upon by both the CE and Kansas Health Information Network, Inc..

Time Frames

1. Kansas Health Information Network, Inc. must provide the written accounting to the CE within the established timeframe as documented in the BA contract or agreement with the CE. The CE must provide the requestor with this accounting or request an extension of time within 60 days of the date the request for the accounting was received.
2. One extension of 30 days is allowed to the CE under the HIPAA Privacy Rule. A request for extension must state the reasons for the delay and the date on which the accounting will be provided to the patient or member. Kansas Health Information Network, Inc. will need to provide any request for extension in writing to the CE per the requirements.

Extension of Privacy Protection to Deceased Individuals	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 019
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.310(b), (c), 164.510 and 164.530(c)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

General rule. The security, privacy, and confidentiality of PHI of patients or health plan members of a CE with whom Kansas Health Information Network, Inc. is, or has been, contracted to perform a service or activity, who are now deceased, will be protected according to the same policies that apply to the PHI of all of the CE's patients or health plan members. This applies to all permitted and prohibited uses and disclosures of PHI.

Personal representatives. An executor, administrator, or other person who has authority to act on behalf of a deceased individual, or on behalf of the individual's estate, must be treated as the individual's personal representative. (See ***Disclosure of Protected Health Information to Personal Representatives*** policy.) However, this only applies to PHI needed by the personal representative in connection with the administration of the estate or other affairs of the decedent.

Exceptions. There are certain exceptions to this general policy that permit additional disclosures of the PHI of decedents. In the following instances, PHI that pertains to deceased individuals may be disclosed without authorization from the decedent's personal representative.

1. Disclosure to coroner or medical examiner. PHI may be disclosed to a coroner or medical examiner for identification of the individual, determination of the cause of death, or as needed by the coroner or medical examiner to perform other duties as authorized by law.
2. Cadaveric organ, eye, or tissue donations. PHI of deceased individuals may be disclosed as necessary to organ procurement organizations, or to others engaged in the procurement, banking, or transplantation of cadaveric organs, for purposes of facilitating the transplantation.
3. Research. A researcher may review PHI of decedents.
   - 3.1. A representation that only PHI pertaining to decedents will be used or disclosed,
   - 3.2. Documentation of the death of each individual whose PHI will be used or disclosed (excepting those individuals for which the CE already has documentation of death), and
   - 3.3. Representation that the PHI sought is necessary for the research.
   - 3.4. Refer Kansas Health Information Network, Inc. policy on Secondary Data Use.

Procedure:

1. All requests for disclosure of PHI to an entity other than the CE for which Kansas Health Information Network, Inc. is contracted to perform a service or activity, will be re-directed to contact the applicable CE. Contact information will be provided to the requestor.

2. Once Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) has been notified by the CE's Privacy Official to release information to another entity for a deceased individual, Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will be responsible to respond to and record disclosures of PHI pertaining to a deceased individual for the following circumstances:

    2.1. To coroners or medical examiners.

        2.1.1. Affected workforce will be trained in the minimum PHI elements that may be disclosed to the coroner or medical examiner.

        2.1.2. This includes information leading to a determination of cause of death or other information required to carry out their other duties as determined by law.

    2.2. If appropriate, affected workforce may disclose PHI prior to, and in reasonable anticipation of, the individual's death.

    2.3. When required by law. Disclosures of PHI of deceased individuals as required by law will be recorded in the same manner as other similar disclosures of PHI that are required by law.

    2.4. Each of these disclosures (2.1- 2.4) above may be considered "reportable" if an accounting of PHI disclosures is requested by the decedent's personal representative. See the "Accounting of Disclosures of Protected Health Information" policy.

3. The Director of Privacy and Data Compliance (DPDC) will assure that all documentation regarding disclosures for deceased individuals of a covered entity, including those that must be recorded in a Disclosure Accounting for the deceased individual, will be retained in Kansas Health Information Network, Inc.'s HIPAA Compliance file and retained for the required six-year period.

Disclosures of PHI for Public Health Purposes	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 020
Section**:** ***Two*** Subject: ***PSO***	Related Law(s): ***45 CFR § 164.512(a), and (b),(1),(i),(iii), and (iv)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

The Privacy Official may authorize the disclosure of protected health information, without the written authorization of the person to whom it pertains, for the following purposes:

1. Routine public health reporting, for purposes of controlling or preventing disease, injury or disability, as required by state law. This includes, (but is not limited to) reporting birth, death, communicable diseases, and certain injuries.
2. Reporting to someone (including a drug manufacturer) under the jurisdiction of the federal Food and Drug Administration (FDA), regarding the quality, safety or effectiveness of regulated products and activities. This includes (but is not necessarily limited to) reporting PHI related to:
    2.1. Adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
    2.2. Tracking FDA-regulated products;
    2.3. Product recalls, repairs, or replacement, or "lookback" (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

Procedure:

1. The DPDC is expected to periodically review its policies and procedures that apply to routine public health reporting to assure compliance with applicable state laws, and to assure that only as much information as is required under such laws is being reported.
    1.1. The DPDC is expected to disseminate information concerning any required changes to current policies and procedures to all affected workers including its BAs who are performing services / functions on their behalf that require the use and/or disclosure of PHI to public health authorities.
    1.2. In these situations, Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC) will discuss with the CE's Privacy Official, methods to assure that changes are promptly incorporated into reporting practices to assure compliance with state laws and to avoid improper disclosure of PHI.
2. The DPDC is expected to periodically review (at least annually) policies and procedures that apply to routine reporting to the FDA (its agents, or others authorized or required by the FDA to receive such information) of adverse events and product tracking information. This review will assure compliance with FDA requirements and assure that only as much information as is required by the FDA is being reported.

3. The DPDC is expected to develop and review procedures to assure that any FDA reporting is related to the quality, safety or effectiveness of FDA-regulated products and activities. For example, it is not permissible to disclose PHI to a manufacturer to allow the manufacturer to evaluate the effectiveness of a marketing campaign for a prescription drug. In this example, although the disclosure may be related to the effectiveness of an FDA-regulated activity (the advertising of a prescription drug), the disclosure is made for the commercial purposes of the manufacturer rather than for a public health purpose.
4. Any disclosure of PHI required as part of a product recall, or to locate or notify patients or health plan members regarding a product recall, will be managed by the DPDC. Care will be taken to assure that only the minimum PHI necessary to protect patients' or health plan members' welfare will be disclosed.
5. The Director of Privacy and Data Compliance (DPDC) will develop a training program for any Kansas Health Information Network, Inc. workforce members or subcontractors who may be affected by such laws in performing services / functions on behalf of the CE, to assure that they are familiar with the provisions of applicable laws regarding public health reporting and know how to apply such laws to disclosures of PHI made under their direction. This training will include providing those Kansas Health Information Network, Inc. workers and subcontractors with a comprehensive list of the public health disclosures that they are authorized to make.
6. When a request for disclosure of PHI for public health purposes is not on the list of disclosures which Kansas Health Information Network, Inc. workers or subcontractors are authorized to make, they will refer the request to Kansas Health Information Network, Inc.'s Director of Privacy and Data Compliance (DPDC). Such disclosures will be reviewed in with the CE's Privacy Officer, General Counsel or other designee.
7. Disclosures made under this policy must be recorded for inclusion in any accounting of disclosures.

Disclosures of Protected Health Information in a Disaster Situation	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 021
Section**:** ***Two*** Subject: ***PSO***	Related Law(s): ***45 CFR § 164.510(b)(4)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Workforce

Policy:

1. Members of Kansas Health Information Network, Inc.'s workforce (employees or subcontractors) may disclose protected health information (PHI) to a public or private entity authorized by law or by charter (such as the local chapter of the American Red Cross) to assist in disaster relief efforts. Such disclosures may be made without the written authorization of the person to whom the information pertains. However, the disclosure may only be for the purpose of coordinating with such entities to locate family members, personal representatives, and others involved in an individual's health care, and/or to notify them of the individual's location, general condition, or death.
2. In a disaster, Kansas Health Information Network, Inc. is allowed to disclose DNA, dental records, and tissue typing, without a court order, to identify victims and locate and notify family members, personal representatives, and others who are involved in their care.
3. Kansas Health Information Network, Inc. workers should attempt to comply with the following, to the extent that, in their professional judgment, doing so does not interfere with emergency response or disaster relief activities:
    3.1. If the individual to whom the PHI pertains is present, or otherwise available, the disclosures of PHI permitted by this policy should only be made in accordance with that individual's desires. The worker may ask the individual if she or he agrees to the disclosure and may give the individual the opportunity to object. The worker may also disclose PHI in accordance with this policy when, based on his or her professional judgment, it can be reasonably inferred from the circumstances that the individual does not object to the disclosure.
    3.2. If the individual to whom the PHI pertains is not present, or otherwise available, or is not capable of giving agreement or making an objection to a disclosure of PHI, a worker may disclose PHI in accordance with this policy when he or she determines that it is in the individual's best interests to do so. A worker may make this determination based on his or her professional judgment.
    3.3. Only the minimum PHI necessary to accomplish the intended purpose of the disclosure may be disclosed.

Procedure:

1. Members of Kansas Health Information Network, Inc.'s workforce (employees or subcontractors) should confer with the Director of Privacy and Data Compliance (DPDC) of Kansas Health Information Network, Inc., and the Privacy Official of the CE, if at all possible, before making any disclosure of PHI in a disaster situation.

2. Any such disclosure must be recorded and reported to the Director of Privacy and Data Compliance (DPDC) of Kansas Health Information Network, Inc. unless the nature of the disaster makes that impossible. When this is the case, the disclosure will need to be reported "after the fact." The information recorded should include:
    2.1. the date of the disclosure.
    2.2. the identity of the member(s) to whom the PHI pertains.
    2.3. a brief description of the PHI disclosed, and
    2.4. the person or persons to whom the PHI was disclosed.
3. Kansas Health Information Network, Inc. workforce members may consult the Director of Privacy and Data Compliance (DPDC) or President of Kansas Health Information Network, Inc., or the Privacy Official for guidance on what information to disclose in a disaster.
4. Disclosures made under this policy must be included in an accounting of disclosures.
5. All documentation regarding the disclosure will be maintained in Kansas Health Information Network, Inc.'s HIPAA Compliance file in an electronic log.
6. Records of disclosures made under this policy will be retained for six years.

Maintenance of Privacy and Security Policies and Procedures	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 022
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.530(i)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: HIPAA Risk and Security Committee

Policy:

1. It is the policy of Kansas Health Information Network, Inc. to implement policies and procedures designed to comply with applicable federal and state *laws* that relate to the privacy and security of *protected health information (PHI)*. Policies and procedures will be changed whenever necessary to comply with changes in applicable laws.
2. All policies and procedures that relate to the privacy or security of protected health information must be retained for six years from the date when they are no longer in force.
3. Kansas Health Information Network, Inc. policies and procedures shall be updated when federal or state law and regulations change or are modified, when Kansas Health Information Network, Inc. adds or deletes services and at other times deemed necessary by Kansas Health Information Network, Inc.

Procedure:

The HIPAA Risk and Security Committee will:

1. Periodically receive updates and/or trade association information to review changes in federal and state laws that relate to the privacy, security, and confidentiality of PHI, and *patients'* rights of access to that information. As a result of these state law changes or changes associated with the Business Associates use of technology and/or operations, necessary changes will be made to Kansas Health Information Network, Inc.'s policies and procedures.
2. Ensure that the changes are reflected in training materials and any other related documents.
3. Periodically monitor compliance with Kansas Health Information Network, Inc. policies and procedures by conducting an annual review of all documentation, revising as necessary to assure documents reflect leading practices for systems, services development and acquisition, implement corrective steps as necessary and ensure such policies and procedures are retained to maintain compliance.

Assignment of Security Responsibility	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 023
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC) and Chief Information Security Officer (CISO)

Policy:

1. Kansas Health Information Network, Inc. recognizes the importance of specialized oversight for the development and implementation of Kansas Health Information Network, Inc.'s security responsibilities. For this purpose, a Director of Privacy and Data Compliance (DPDC) who is a workforce member of Kansas Health Information Network, Inc. and has been designated with the assigned responsibility to develop, implement, manage and monitor the execution, use and effectiveness of a consistent entity-wide Privacy, Cyber Security/Security Data Protection Program. The Director of Privacy and Data Compliance (DPDC) is qualified for the role by sufficient years of experience and related industry recognized certifications and continuing education. The Privacy Security Officer works closely with other senior level representatives including but not limited to the Chief Information Security Officer and Human Resources to assure cybersecurity is included in human resource practices such as personnel screening and deprovisioning. Duties shall include, but not be limited to, the following:

    1.1. Establish entity wide security management structure. This includes the development of a documented and current Security Program or Plan including the following components at a minimum:

        1.1.1. Develop, implement, and oversee the Security Management Process including Risk Analysis and Risk Management provisions. Security Management Process refers to creating, administering, and overseeing policies to ensure the prevention, detection, containment, correction, evaluation of risk and mitigation of security breaches. The requirement for this process includes the use of risk analysis and risk management, and must include formal security, information system activity review, and sanction policies.

        1.1.2. Oversee process for systems evaluation: The technical evaluation that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of technical and non-technical security requirements. This evaluation may be performed internally or by an external accrediting agency.

    1.2. Coordinate development and execution of the Kansas Health Information Network, Inc. *contingency plan*: A contingency plan may include:

        1.2.1. Applications and data criticality analysis.

        1.2.2. A data backup plan.

        1.2.3. A disaster recovery plan.

        1.2.4. An emergency operation plan, and

        1.2.5. Testing and revision procedures.

2. Unify and oversee information access control standards including assisting management in assigning appropriate system access to data.

   2.1. *Access* refers to the ability or the means necessary to read, write, modify, *or* communicate data/information or otherwise make use of any system resource.

   2.2. *Access control* refers to a method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day access and classification or role-based access.

3. Monitor internal *audit controls* of system records activity and respond to variances. *Audit controls* refer to mechanisms to record and examine system activity. This includes recording pertinent data relating to the creation, modification, transmission, deletion of records, and access to sensitive records, including access log monitoring. Sensitive records include records of employees and VIPs, or records of *members* with protected diagnoses such as HIV or mental illness. Audit controls may also include procedures to monitor access to a statistical sample of all records. Audit controls allow an organization to identify suspect data activities and respond to potential weaknesses.

4. Maintain and manage personnel *authorization controls* and clearance records. *Authorization controls* refers to a mechanism for obtaining consent within the system for the use and *disclosure* of health information. These controls may be role-based or user-based.

5. Oversee Security Configuration Management. Develops, documents, and implements a configuration management plan that details the scope, role, responsibilities, and ensures management commitment to ensure compliance of Configuration Management (e.g., through policies, standards, processes). The integration process to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses.

6. Oversee Incident Response procedures. Security Incident Procedures refers to the requirement to implement formal, documented instructions for reporting and responding to security breaches.

7. Coordinate initial access management, termination and/or modification of *access* to information systems.

8. Oversee Malicious Software Infrastructure. Ensure Kansas Health Information Network, Inc. wide anti-virus infrastructure is in place and operational.

9. Provide technical assistance for universal security awareness training.

10. Develop and oversee Device and Media Controls. The entity is required to have a policy for formal, documented policies and procedures that govern the receipt, removal, and storage of data storage media into and out of a facility. They are important to ensure total control of media containing health information.

11. Assess and monitor ongoing compliance with Security policies and procedures including addressing new requests for data.

12. Perform first level trouble shooting for security and security related issues. This includes appointing security contacts by name and in writing for each major organizational area or business unit.

13. Oversee a routine and periodic technical and non-technical (operational) review of all of Kansas Health Information Network, Inc.'s policies and procedures resulting from the initial risk analysis and general risk management program. This initial evaluation will take into consideration the initial enterprise status of the Business Associate and its resulting early interpretation of the Administrative Simplification Security components. This will be Kansas Health Information Network, Inc.'s benchmark evaluation. Moving forward, the same routine evaluation will occur and result in changes to the HIPAA Security Policies and Procedures as necessary.

Risk Analysis and Ongoing Risk Management	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 024
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a) (1) (ii) (A) & (B)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: HIPAA Risk and Security Committee

Policy:

1. Kansas Health Information Network, Inc. recognizes the importance of the risk analysis and risk management functions. As such, it has focused time and resources to develop a formal methodology to set forth an effective risk management process involving appropriate individuals. Risk management validates the effectiveness of chosen policy and/or solutions serving to balance the protection of confidentiality of electronic protected health information with the ability to make it available to support the health care process. The privacy, security and risk management program(s) is/are updated to reflect changes in risks.
2. Risk Management includes three components:
   - 2.1. Risk Assessment- The process to determine level of risk.
   - 2.2. Risk Mitigation- The process to decrease the determined level of risk.
   - 2.3. Evaluation and Assessment – The process to monitor and take action to maintain the decreased level of risk. The HIPAA Risk and Security Committee will conduct an initial, comprehensive risk analysis to be used as a benchmark for ongoing risk management and evaluation activities. The initial risk analysis includes the following components at a minimum:
     - 2.3.1. Baseline development and value determination covering Administrative, Physical, and Technical requirements.
     - 2.3.2. Determination of the level of reasonability and scalability for Kansas Health Information Network, Inc. by weighing size, complexity, organization capabilities, cost, technical capabilities, probable threats and related costs.
     - 2.3.3. Review and further assessment of addressable requirements.
3. Ongoing risk management includes the following components at a minimum:
   - 3.1. Methodical evaluation and determination of process(s) and/or technical solution(s) designed to address each Security requirement, while balancing the confidentiality, integrity and availability of protected health information.
   - 3.2. Managing a realistic implementation of the process(s) and/or technical solution(s) via formal Change Control.
   - 3.3. Documenting in policy and procedure form all processes/technical solutions.
   - 3.4. Incorporating any necessary information in training materials.
   - 3.5. Managing the necessary workforce training.

3.6. Creating and performing ongoing audits or evaluations of the chosen process(s) and/or technical solution(s) in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the protected health information with its integrity and availability.

Procedure:

1. The HIPAA Risk and Security Committee has the combined responsibility of privacy and security oversight. This oversight includes the following.
   1.1. Review of Kansas Health Information Network, Inc. and cataloguing of all gathered documentation for ease of reference in future evaluations.
   1.2. Taking necessary actions to reduce risk associated with the security topic that may include:
      1.2.1. Doing nothing: This will occur If Kansas Health Information Network, Inc. believes the current safeguards provide an acceptable level of risk.
      1.2.2. Reducing or mitigating: This process allows for the implementation of new integrated safeguards/controls that function to further protect the asset and/or lower the risk level using different control types (layered, preventative, detective, corrective and compensating).
      1.2.3. Transferring the risk: This process allows for the risk to be transferred to another organization such as by purchasing insurance or choosing a more secure method for a business process (e.g. transcription).
   1.3. Reviews and maintains records of compliance results (e.g., organization-defined metrics) in order to better track security trends within the organization, respond to the results of correlation and analysis, and address longer term areas of concern as part of its formal risk assessment process.
2. The first component of the risk analysis process is to gather documentation related to the current processes safeguarding electronic protected health information. Based upon information available, this may include:
   2.1. Administrative Safeguards and workforce policies and procedures relating to electronic information. Examples may be:
      - Security/Confidentiality Statements.
      - Employee handbook.
      - HIPAA/HITECH Privacy, Cyber Security and Security training materials.
      - Sanctions Policies.
      - System Use Auditing or Reporting Activities.
      - Emergency workforce contact information.
      - Business Associate or Trading Partner Agreements.
      - Current Disaster Recovery Plans.
      - Current Safety Policies and Procedures.
      - Current emergency resource contact lists or other emergency mode documentation.
   2.2. Physical Safeguards or physical measures designed to protect buildings and equipment where information systems are housed. Examples may include:

- Blueprint or layout of physical buildings, support structures, wall, door and ceiling construction.
- Related workforce clearance/access ability to physical premise.
- Lists of keys, codes, or swipe card access to building.
- Fire prevention and protection system documentation.
- Inventory of all hardware, software, portable devices, media and
- Inventory of all physical structures containing equipment.
- Policies and procedures governing workstation location and security.
- Disposal, Reuse, and Accountability procedures for devices and other media.
- Potential security threats by neighboring premises.

2.3. Technical Safeguards

- Cyberthreat Intelligence (received from information sharing forms and sources).
- Network diagrams including location and configuration of firewalls, servers, dial-up connections and routers.
- Technical vulnerability scans (penetration scans of information systems, hosted applications, virtualized environments, and related configuration) which serve to monitor, assess, rank and allow for remediation of system identified vulnerabilities/threats including cyber security threats. Vulnerability scanning is used to evaluate the potential threats to all information system components supporting PHI. This includes, but is not limited to applications that store, process or transmit PHI. Regular penetration testing should be conducted from outside and inside the network perimeter on a routine (monthly basis). Findings should be reviewed, mitigated as necessary in accordance with Change Control procedures. At least once every three hundred and sixty-five (365) days an independent review should be conducted by a qualified party which includes tests for the protection of unprotected system information which would be useful to attackers.
- Vendor contact information and documentation of software and hardware.
- Policies and procedures defining electronic access privileges including initial authorization, establishment and termination.
- Audit and Integrity Controls.
- Authentication of person or entity.
- Controls for transmission security.

2.4. Documented flow of PHI from initial creation to use and disposal**.** This may include form and content of all systems, subsystems, databases and names and be in the form of flow charts or hand drawings.

2.4.1. PHI is encrypted when stored/maintained in non-secure areas. If it is determined that encryption is not reasonable and appropriate, the factors used to make that decision are documented along with the acceptance of such risk.

2.5. List of all organizational assets, including the estimated value of each asset. The estimated value will include the actual value and the replacement value of the asset if it were lost.

Unique Factors Determine Level of Reasonable and Scalability

3. All information gathered is then considered in accordance with the following factors:

3.1. Size, complexity and capabilities of covered entity.

3.2. Technical infrastructure, hardware, software, and security capabilities.

4. Costs of security measures.

5. Probability and criticality of potential risks to electronic protected health information. Potential risks or threats need to be thoroughly evaluated.

5.1. Use the "HIPAA Security Addressable Worksheet" to document all decisions related to addressable items. The worksheet provides a mechanism for the Business Associate to document the following:

5.1.1. For those implementation specifications identified by the regulators as addressable, consider the following:

- The Kansas Health Information Network, Inc. general risk analysis responses.
- Current measures in place.
- Applicability to size of organization.
- Cost of implementation.

5.1.2. Document the following for each:

- Based on the above factors Kansas Health Information Network, Inc. has chosen to implement the specification due to the fact that it is reasonable and appropriate or;
- Based on the above factors Kansas Health Information Network, Inc. has chosen to implement an alternative security measure to accomplish the purposes of the standard or;
- Based on the above factors Kansas Health Information Network, Inc. chooses not to implement anything if the specification is not reasonable and appropriate and the standard can still be met.

5.2. Review the results of technical compliance checks, performed by experienced specialists with the assistance of automated software tools. SEE Activity Review of Information System Security Policy and Procedure.

6. The HIPAA Risk and Security Committee will oversee the performance and documentation related to the risk analysis project. All information gathered whether created manually or via automated tools (preferred and used whenever possible), will be organized, maintained securely and retained in accordance with Kansas Health Information Network, Inc. documentation policies (at least six years from the initial date of creation or the date when it last was in effect whichever is greater). While ongoing risk analysis may be conducted via internal resources, on a routine basis, an independent review will occur in order to assure ongoing compliance and effectiveness of Kansas Health Information Network, Inc.'s Privacy, Cyber Security and Security Data Protection Plan. Those who conduct ongoing assessment must possess appropriate credentials and maintain a level of independence in order to objectively and fairly provide feedback.

7. Risk Designations will be defined for each function/role across Kansas Health Information Network, Inc., reviewed at least annually and include screening criteria as a tool to mitigate the risk of Kansas Health Information Network, Inc. having key positions filled with qualified resources.

8. If teleworking is used, additional insurance shall be in place to address the risks of teleworking.

Risk Mitigation

9. The HIPAA Risk and Security Committee will assure the results of internal and external risk analysis are appropriately communicated and reported to senior management/President for approval and that

Kansas Health Information Network, Inc. has acceptable level of risk and mitigation (corrective action) plans for any findings are handled.

10. The HIPAA Risk and Security Committee will additionally ensure that any and all related policies and procedures will be updated, including training materials.
11. The HIPAA Risk and Security Committee will organize all information gathered during this process, maintain it securely and retain the information in accordance with Kansas Health Information Network, Inc. document retention policies. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications.
12. The HIPAA Risk and Security Committee) will ensure that routine monitoring (ongoing risk evaluation and assessment) of this solution is carried out at least annually and more frequently if resulting from a significant change in business, operations or information systems in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the protected health information with its integrity and availability. Longer term comparisons of findings and result provide correlation and analysis perspective. Kansas Health Information Network, Inc. updates the risk assessment before issuing a new formal authorization to operate or within every three years, whichever comes first when conditions occur that may impact the security or authorization state of the system.

Vendor/Third-Party Supply Chain Risk Management	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 025
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.312 & 164.308*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Technology Vendor Review Committee, Operations, Legal/Compliance and Systems support as necessary

Policy:

1. The Director of Privacy and Data Compliance (DPDC) is responsible to establish a Technology Vendor Review Committee consisting of business, operations, legal/compliance and technology representatives to conduct general oversight of Kansas Health Information Network, Inc.'s data sharing related to third parties/vendors. This oversight includes the following:
    1.1. Establishing a method to allow Managers to request third party/vendor assistance which requires documentation of the type of service requested including but not limited to the period of time requested, the level of PHI to be handled and other business and contractually related items. Kansas Health Information Network, Inc. always employs the highest ethical standards in its business practices including source selection, negotiation, administration, and determination of purchasing and contracting activities. The process is applied when acquiring systems or services and includes maintaining security during transitions and continuity following a failure or disaster. Additionally, the process must:
        1.1.1. Allow for detailed information to be gathered regarding the downstream/third parties handling of PHI including but not limited to the implementation of policies and procedures, administrative, physical and technical safeguards and ongoing certifications/accreditation maintained.
        1.1.2. Include a method to weigh the importance of the activity for Kansas Health Information Network, Inc. along with the level of data to be handled.
        1.1.3. Allow for the due diligence to be conducted initially upon the commencement of the relationship/contract execution (prior to trading PHI) and to set forth regular intervals for ongoing monitoring of Service Level Agreements and privacy and security compliance of identified security requirements throughout the life cycle of the relationship.
        1.1.4. Includes specific security-related requirements in information system acquisition contracts based on applicable laws, policies, standards, guidelines and business needs.
    1.2. Establishing a model for vendor management, including measurement of performance, service delivery, service level agreement, and other contracted items.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will oversee the Technology Vendor Review Committee responsible for defining the preferred process and/or technical solution(s) to address Vendor Management and decrease or mitigate the associated level of risk associated with contracting and sharing PHI with third parties.

2. A method to capture the desired service request including key information of service delivery expectations including but not limited to the level of data to be shared/accessed is first implemented to assure efficient supplier service is met across Kansas Health Information Network, Inc..
3. The following factors are to be considered during this process:
   3.1. Initial risk assessment results and related documentation.
   3.2. Various other factors including organization size, complexity, capabilities, cost and probability of threat to the protected health information.
   3.3. All areas defined in these templates as “Implementation Considerations”.
   3.4. Investigation of technical solutions or products designed to meet the goals of the policy (for example a simple spreadsheet may be used to track the due diligence and ongoing monitoring process, or an automated risk management tool may be used).
   3.5. The ability for the process and/or technical solution to balance the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
   3.6. Access to Kansas Health Information Network, Inc. information and systems by external parties is not permitted until due diligence (screening of privacy/security and other controls) has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting specific obligations for privacy and security requirements (terms and conditions) is signed acknowledging they understand and accept their obligations. Minimal electronic/system and/or physical/facility (badge) access is provided after the contractor/vendors ability to comply with privacy and security requirements has been established.
4. Once a process is implemented, the committee is also responsible to create, disseminate to its workforce and annually review/update a list of current service providers including a description of the services provided. Kansas Health Information Network, Inc. documents all existing outsourced information services and conducts an organizational assessment of risk prior to the acquisition or outsourcing of information services.

Implementation Considerations:

Due Diligence Prior to Contracting –Risk Weighting

A screening process is carried out for third parties to assure privacy/security safeguards are in place, aid in the fair selection process and set forth a method to continuously monitor the services.

- Due diligence of the external party takes place prior to contracting and may include interviews, document review, checklists, certification reviews (e.g. EHNAC/ HITRUST) or other means to validate the third party complies with industry/government standards.
- The identification of risks related to external party access takes into account a minimal set of specifically defined issues. A checklist, scorecard or automated tool is recommended to assure third party measurements are applied consistently across all considered for contracting. Specific cyber security risks are addressed.
- Kansas Health Information Network, Inc. identifies and mandates information security controls to specifically address supplier access to Kansas Health Information Network, Inc.'s information and information assets.
- Reference checking including those provided and previous customers.
- Review of federal/state exclusion and sanction lists (as applicable).
- Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls are reconsidered prior to purchasing the product.

Assuring Safeguards are in Place Prior to Sharing of PHI

Written agreements with third parties may also include the following:

- An acknowledgement that the third party is responsible for privacy and security of the data and requirements to address the associated information security risks and requirements associated with communications technology services (e.g., cloud computing services and/or specific functions, ports and protocols to be used) and product supply chain.
- Specific responsibilities for the protection of covered information shared.
- Specific limitations of access, arrangements for compliance auditing, penalties, liability, indemnification, and requirements for notification of third-party personnel transfers and terminations.
- Required security controls designed to detect, prevent, and mitigate risk. including personnel security, including roles and responsibilities for third-party providers aligned with internal security roles and responsibilities.
- Where software development is outsourced, formal contracts address the ownership and security of the code and application.
- Where collection and disposal services are offered for secure media disposal, care is taken to select a suitable contractor with adequate controls, experience, and a written agreement to ensure the risk of information leakage to unauthorized persons is minimized.
- Potential restriction on the location of facilities that process, transmit or store covered information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual, and other security and privacy-related obligations.
- If assets are assigned to contractors and/or volunteers, written procedures for assigning and monitoring use of the property should be included within the contract and/or Acceptable Use document which is signed by all parties and includes agreement on how and when the property will be inventoried and returned upon completion of the assignment.

Ongoing Monitoring

Routine monitoring occurs as follows:

- Regular progress meetings are conducted, and minutes are taken on an ongoing basis.
- An annual review is conducted which includes review of reports, audit trails, security events, operations issues, failures, and disruptions and to assure problems/issues are appropriately documented and mitigated in accordance with agreed upon Service Level Agreements.
- Network service features and service levels to detect abnormalities and violations are specifically reviewed and formally managed.
- Should software development be outsourced, the development process is monitored and includes independent security and code reviews.
- User IDs assigned to third parties are reviewed at least annually in accordance with Access procedures.

- Where additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls.

5. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will work to ensure the various related implementation subtasks are based on a realistic implementation time. This includes initial implementation of the third-party contract and then on an ongoing basis to verify continued enforcement of privacy and security obligations by third parties.
6. The Director of Privacy and Data Compliance (DPDC) will additionally ensure that any and all related policies and procedures will be updated, including training materials.
7. The Director of Privacy and Data Compliance (DPDC) will organize all information gathered during this process, maintain it securely and retain the information in accordance with Kansas Health Information Network, Inc. document retention policies.
8. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the protected health information with its integrity and availability.

Activity Review of Information System Security	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 026
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a) (1) (D)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO)

Policy:

Kansas Health Information Network, Inc. maintains an internal privacy and security data protection/control program complimented by the electronic access privilege (user authentication) process acting as a deterrent to internal abuse by making users aware that audit trails, physical access reports, file access reports, cyber security and security incident tracking reports are produced, reviewed, investigated on an as needed basis.

1. According to operating system and application capabilities, routine review of information systems activity provides an automatic trail or log or trace of user actions whenever sensitive or critical protected health information is accessed or modified by a workforce member. Together, the audit log, file access reports and security incident reports promote individual user accountability and allow Kansas Health Information Network, Inc. an ability to reconstruct significant events or suspicious activities as necessary.
2. Documentation of routine review of information systems activity for Kansas Health Information Network, Inc. may use manual and technical tools including but not limited to the following:
    - 2.1. Physical access reports.
    - 2.2. Hard copy reports are destroyed as soon as feasible.
    - 2.3. Electronic systems allow for automated tools and reports regarding the Change, Review, Update/Addition and Deletion of PHI.
    - 2.4. Information Protection Systems (IPS) and/or Intrusion Detection Systems (IDS) are in place and used for reporting information security events.
    - 2.5. Historic vulnerability audit logs are reviewed to determine if high scan findings identified within the information system have been previously exploited.
    - 2.6. A centralized, mobile device management solution is in place on all mobile devices allowed to store, process and transmit PHI.
    - 2.7. Unauthorized connections of mobile devices are monitored.
    - 2.8. Upon at least an annual basis (more often if changes), a review/check on the technical security configuration of systems either manually, or via automated tools is undertaken.
    - 2.9. Billing systems allow for reports of activity on deleted charts and payments. On a monthly basis, billing information is reconciled, and any suspicious activity reviewed in depth.
    - 2.10. Systems allow for auditing of PHI and related activity. This includes a record of activity by user, note and date of note.

2.11. Online storage of audit logs, file access reports and security incident reports in a secure manner and for a specified period of time.

2.12. Automated warning messages that appear prior to a user accessing certain sensitive information.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will continue to review capabilities of all systems (including, but not limited to networking, operating and application systems) to ensure access reporting and other necessary user activity is reported as necessary for the Business Associate.
2. The Director of Privacy and Data Compliance (DPDC) will work with others to implement technical processes to support audit trails and other forms of system activity review. These include but may be expanded to include more than Intrusion Detection, Information Protection Systems, Mobile Device Management Solutions, Vulnerability Scanning and routine Systems Access Reviews. This includes updating any and all related policies and procedures and training materials.
3. The Director of Privacy and Data Compliance (DPDC) will conduct or coordinate any necessary training for affected workforce members.
4. The Director of Privacy and Data Compliance (DPDC) will ensure that monitoring of this solution is carried out on a routine basis in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the protected health information with its integrity and availability. This routine monitoring also includes review of new technologies in order to more specifically define, capture and retain ongoing review of system activity information.

Assignment and Management of Information Access Privileges	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 027
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a)(3), (a)(4)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO), Chief Operating Officer (COO)

Policy:

Workforce Clearance and Authorization Access Profiles

1. Kansas Health Information Network, Inc. utilizes Role Based Access Controls (RBA-C) to restrict system access. Each job description is associated with a RBA-C profile, that defines the permissions and privileges to enable access necessary for the documented role and responsibilities.
2. RBA-C profiles includes documentation on role level access to sensitive information, including and not limited to PHI. These profiles will specify the data elements that comprise PHI.
3. RBA-C profiles are based upon two principles: First, that access to information must not be so restricted as to interfere with the efficiency of operations or the quality of services. Second, that access must be sufficiently restricted to afford individuals as much privacy and security as possible.
4. RBA-C profiles are used to limit electronic access to protected health information and comply with the Privacy Minimum Necessary Rule. This includes restricting access to privileged functions and all security-relevant information.

    4.1. RBA-C profiles define the level access for each application/system, which map to permissions and privileges within each application/system. Levels permissions and privileges for each of the an application/systems owner including the level of sensitivity and inclusion of PHI. This includes hardware, software, firmware and may be event-by-event basis, by functional role (user/administrator) and documented for each product line/systems/element/menu. Pre-approved permissions based on the RBA-C and manager approval is defined in 'Process: Internal Request Processing'. The sensitivity of applications/systems is explicitly identified and documented by the application/system owner.

    4.2. RBA-C profiles create a mapping each user to one or more roles and each role to one or more systems.

    4.3. Elevated privileges to provide additional permissions and privileges for a defined task, beyond the assigned RBA-C profile. Elevated privileges are requested and managed for specified timeframes necessary for the defined task, including start and end dates. Elevated privileges are limited to a pre-defined subset of users, assigned to a different user ID versus normal business use; in a single role and only as minimally necessary.

        4.3.1. Based on business need, Supervisors are responsible for extending or ended Elevated privileges.

    4.4. Access to administrative functions/consoles for hosted/virtualized systems are restricted based on "least privilege" via policy and technical controls.

Access Establishment and Modification

1. Kansas Health Information Network, Inc. has created a documented process to grant or initially establish access profile information (allowing or establishing access to certain physical areas, technical applications, and electronic data).
2. As part of creating a new job description, the supervisor assigns or drafts a RBA-C consistent with documented responsibilities.
3. RBA-C profiles are reviewed annually.
    3.1. The supervisor is responsible for reviewing.
        3.1.1. The responsibilities of the role.
        3.1.2. If changes are needed (expanding or removing access) from changed responsibilities.
    3.2. Any changes are cross reviewed by the DPDC and presented to the HIPAA Risk Assessment Commitment for final approval.
4. RBA-C profiles may be modified for members of the workforce who have a demonstrated need to use/access additional information to accomplish their work assignments. This includes hardware, software, firmware and may be event by event basis by functional role (user/administrator) and documented for each product line/systems/element/menu. In such a situation, the supervisor requests the modification and final approval is given by the Privacy and Security Officer.
5. If a member of the workforce no longer requires access to a particular information profile, then that modification or termination of access privileges by disabling and/or removing accounts will be requested by the supervisor. DPDC Director of Privacy and Data Compliance (DPDC).

Procedure:

1. The Chief Operating Officer, or delegate, is accountable for managing and maintaining the RBA-C documentation. The RBA-C documentation includes the system/application level of access, access to information, and a mapping of the job description to the RBA-C Profiles. Director of Privacy and Data Compliance (DPDC).
2. Application owners are responsible will define and informing any changes to level of access within the system.
3. Supervisors are responsible for:
    3.1. Create Access Profiles. Create the access profile by reviewing job descriptions and assigning them to job classes based on the PHI required to accomplish the job efficiently.
        3.1.1. User identities are verified prior to the establishment of an account.
        3.1.2. Relevant policies and procedures and a written statement of access rights are reviewed, and user acknowledgement is gained prior to access being granted.
        3.1.3. Guest/anonymous, shared/group, temporary and emergency accounts are specifically authorized and monitored.
4. The Privacy and Security Officer (DPDC) is responsible for:
    4.1. Develop the Policy and combined Technical Solution. Determine the Kansas Health Information Network, Inc. preferred combined policy and technical solution to perform workforce clearance and authorization access, establishment and modification procedures by considering the following:
        4.1.1. Reviewing the risk assessment results, auditing, and related documentation.

4.1.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

4.1.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.

4.2. The Director of Privacy and Data Compliance (DPDC) is responsible for authorizing all RBA-C profiles.

5. The Chief Information Security Officer is responsible for:

5.1.1. Investigating and implementing technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

6. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of access profiles and the technical solution utilized to establish and modify such profiles occurs on a routine basis. This includes:

6.1. Audit review of access profiles:

6.1.1. User access rights are reviewed after any changes and reallocated as necessary.

6.1.2. Critical system accounts and privileged access rights are reviewed at least every 60 days.

6.1.2.1. All other accounts including user access and changes to access authorizations are reviewed at least every 90 days. Old accounts are closed after (within) 90 days of opening new accounts.

6.2. Monitoring members of the workforce have electronic access to PHI that is consistent with their access profiles. A documented list is maintained in RBA-C documentation.

7. Internal Access Change request and other user permission tickets are used to request and track user permissions.

Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 028
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a)(3)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO) Workforce

Policy:

Kansas Health Information Network, Inc. will terminate access to information systems and other sources of *protected health information* (PHI), when an employee, agent, or contractor ends his/her employment or engagement. Kansas Health Information Network, Inc. will terminate access to specific types of PHI when the status of any business associate or member of the workforce no longer requires access to those types of information.
The Director of Privacy and Data Compliance (DPDC) receives, acts upon and documents notices of all terminations or modifications of access to the building and computer system.

Procedure:

1. Upon termination of employment, contract or assignment requiring a particular level of access authorization, the Director of Privacy and Data Compliance (DPDC) or designee will immediately complete a Notice of Termination or Modification of Access form (Notice). Automated mechanisms to facilitate the efficiency and communication of the termination/change will be used as deemed appropriate based on [BUSINESS ASSOCIATES] operating size and complexity of systems.
    1.1. The Notice will include the individual's name, job function, access site, known information access rights, a description of the modifications to access required by the change in status and date that the termination or modification is effective.
        1.1.1. Should the terms of the exit and/or workforce member's situation for leaving be considered high risk, physical/logical access rights will be immediately removed or modified, and the subject person will be escorted from the site as determined necessary.
2. The Director of Privacy and Data Compliance (DPDC) or designee will initiate the process of access termination or modification in the relevant information system(s) as well as the following steps as deemed necessary to maintain overall systems' security. Access will be restricted within 24 hours of receipt of notice and the following actions will be taken:
    2.1. Retrieving Keys, Tokens, or Cards that Allow Access.
    2.2. Removal or Modification of User Accounts.
    2.3. Reminding exiting employees: Prior to the final exit of an employee, he or she should be reminded of and should review any non-disclosure or employment agreements that have been signed. The employee should be reminded that any PHI received during employment still falls under these agreements.
3. On a routine basis, the Director of Privacy and Data Compliance (DPDC) or designee will review recent terminations and/or modifications of computer or building access to determine that the process is working efficiently and in a timely manner.

Disaster Recovery and Business Continuity Plan	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 029
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.308(a)(7)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Executive Officer (CEO), Chief Operating Officer (COO)

Policy:

1. The Kansas Health Information Network, Inc. Risk Management policy defines disaster recovery and business continuity planning as an integral component of overall security. Kansas Health Information Network, Inc. maintains a comprehensive Disaster Recovery and Business Continuity Plan in order to ensure that electronic protected health information is available, secure and has not been changed or tampered with (consistent integrity). Kansas Health Information Network, Inc. addresses Disaster Recovery/Business Continuity issues in a timely manner.
2. In general, the Disaster Recovery and Business Continuity Plan provides a mechanism for Kansas Health Information Network, Inc. to accomplish the protection of the following assets in response to negative and unexpected occurrences while minimizing the total impact on business operations in response to the crisis:
    2.1. Protect lives and personal safety.
    2.2. Protect sensitive data and allow for information safety and recovery.
    2.3. Protect equipment, limit damage and allow for recovery.
    2.4. Protect the Facility, limit damage and allow for recovery.
    2.5. Specifically, the Disaster Recovery and Business Continuity Plan provides a mechanism to:
        2.5.1. Minimize impact on total business operations, minimize interruptions to critical functions so that they occur only infrequently, are brief in duration, and do not result in detrimental consequences.
        2.5.2. Address complications and consequences of normal lost processing time, operations degradation, lost equipment replacement processes, insurance funds, alternative processing sites, temporary office space, equipment, key personnel, telephones and other business basic equipment.
3. The CEO and COO Director of Privacy and Data Compliance (DPDC) and other workforce as applicable are responsible to create, obtain management approval for, implement, and maintain a comprehensive Disaster Recovery and Business Continuity Plan including the following components:
    3.1. Data Back-up Plan: Provides for the creation and maintenance of an exact retrievable copy of all Kansas Health Information Network, Inc. electronic protected health information. It may also include maintenance and retrieval of paper files of protected health information.
    3.2. Disaster Recovery Plan: Defines procedures to restore any loss of data and equipment due to an emergency, power loss, fire, vandalism, natural disaster or other occurrences.

3.3. Emergency Mode Operation Plan: Allows for continuation of critical business processes for protection and security of PHI even during emergency mode/alternative processing operations.

3.4. Testing and Revision: Allows for routine testing of contingency plans as necessary in accordance with Kansas Health Information Network, Inc. system complexity and other factors reviewed during the Risk Analysis and Risk Management Process. This includes but is not limited to the proof of restoration meeting the RPO and RTO published timelines.

3.5. Applications and Data Criticality: Based upon system complexity and importance as a result of Risk Analysis and Risk Management, this process allows for the prioritization of system applications and related data in order to support resumption of normal business/systems processing.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to all areas of contingency planning. This ensures that the processes chosen to carry out the contingency planning policy are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc.

1.1. The Director of Privacy and Data Compliance (DPDC) and other workforce members as applicable are charged with choosing the Kansas Health Information Network, Inc. preferred combination of process and solution(s) to perform Disaster Recovery and Business Continuity Plan by considering the following factors:

- Reviewing the risk assessment results and related documentation including but not limited to,
- The identification of business processes, related technology needing Business Continuity/Disaster Recovery Planning; Identified threats; Business Impact Analyses (to evaluate the consequences of negative events).

1.1.1. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

1.1.2. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.

1.1.3. Thoroughly considering all areas defined below as “Implementation Considerations.”

Implementation Considerations for Disaster Recovery and Business Continuity Procedures

Planning Phases - The initial phases of Disaster Recovery and Business Continuity Plan must include basic planning components such as:

- Definition/Plan Scope
- Background
  - Functional Requirements and Assumptions
  - Team(s)/ Team Members
  - Emergency Response Team
- Design and Development of the plan
  - Function List and Priority Assignment
  - Backup
  - Vital Record identification and Protection
  - Recovery Strategies, contingency Strategies, and recovery Locations
  - Document Procedures
  - Testing and Document Revision

- Implementation
- Testing
- Monitoring
- Maintenance

A. Level of Emergency Response

In an unexpected event such as a fire, loss of electricity, vandalism or other disaster Kansas Health Information Network, Inc. usual security measures may become disabled or may be ignored or not observed by workforce members. Therefore, responses must be preplanned, communicated, and documented in training materials so that workforce can carry out a series of actions and reactions that range from manual to highly complex processes. Based upon level of functional loss (short term disruption of computer systems versus projected number of days in alternative working site), various responses will be performed: All actions will result in maintaining the ongoing operations of those functions deemed most critical to Kansas Health Information Network, Inc.

B. Prioritize Actions Based on Probability

The Director of Privacy and Data Compliance (DPDC) will work with others to develop a list of possible threats that have a certain probability of occurring on-site. The level of probability that will trigger a specific level of contingency plan is a component of the Risk Analysis and Management process. However, some more common threats ranging in probability from high to low may include:

- Computer System disruption in connectivity resulting in delayed processing time or rework.
- Loss of electrical power, lights, telephones and other office equipment due to thunderstorm, power outage and other such natural events.
- Fire, earthquake, tornado or other disaster where all or part of the actual facility is destroyed, resulting in need to set up temporary work location.

C. Data Back Up Plan

1. Kansas Health Information Network, Inc. requires the creation and maintenance of an exact retrievable copy of Kansas Health Information Network, Inc.'s electronic protected health information. A documented definition including the workforce member(s) accountable to prepare backups including the level of backup required for each system, specific scope, duration and frequency of imaging and retention of such image is in place. As such, back-ups which include the data and systems configuration/software, are created in the most appropriate form and encrypted (this may include, but is not limited to tapes, CD ROM, RAID, SANS, SFTP copy, etc.) and in a timely manner. Automated tools are used to create and track all back-ups. Inventory records for the backup copies, including content and current location, are appropriately maintained.
2. Kansas Health Information Network maintains a full back up of all data in the Microsoft Azure Cloud and the Amazon Web Services cloud. These are updated daily.
3. Routine restoration procedures are regularly performed to assure data and systems can be restored in accordance with the plan.
4. In the instance that back-up data is used to restore system operations, the Director of Privacy and Data Compliance (DPDC) will reset all system defaults with assistance from System.

D. Disaster Recovery Plan- Required Procedure to Restore Loss of Data

The Director of Privacy and Data Compliance (DPDC) will compile and maintain the information outlined below to be stored in multiple formats on and off site (remote site) to be used in the event of an emergency. This critical Disaster Recovery Plan Outline includes a description and designated

ownership with clearly defined responsibilities for the orderly resumption of activities and resumption of system recovery to the point of failure. It includes an outline of the business priorities for Kansas Health Information Network, Inc., including related assumptions and a final base plan with activation criteria (based on those business priorities). Establish Comprehensive Lists.

1. List of workforce members deemed responsible to carry out response contingency processing (include name and emergency contact information), and
    - Inventories.
    - List of back-up systems/data, location and contact information and contracts including alternative storage and processing sites at a sufficient distance.
    - Critical forms and supplies stocked off-site.
    - List of reliable resources for equipment replacement.
    - Processing priorities pre-approved by management. (Sequence of importance of each application).
    - System application and documentation (current copies of all applications need to be located on and off site in a secure manner) SEE EMERGENCY ACCESS PROCEDURES.
    - Testing and Revision Plans.
    - List of job categories and/or individuals responsible for recovery of computer and other systems. Job categories may include restoring operations, and/or retrieving previously backed-up data.
    - List of all critical business partners and emergency contact.

E. Emergency Mode Operation Plan

Kansas Health Information Network, Inc. requires defined processes to protect electronic protected health information during and immediately after a crisis while operating in emergency mode. Basic elements include definition of the notification process, clear pre-defined instructions on work around procedures, crisis management information and business continuity planning. This may include administrative safeguards, physical safeguards and access of workforce to site (or alternative sites), limitation of electronic and other technical safeguards including access via "Electronic Access Control" to protect and secure protected health information even during emergency mode operations. This most likely includes adequate manual processes for use until automated operations are restored.

F. Testing and Revision

Based upon Risk Analysis results and system and configuration complexity, each component of the Contingency Plan is identified, evaluated and prioritized for necessary routine testing and adjustment or revision. Recovery Time Objectives and Recovery Point Objectives (in less than 48 hours) are defined and published as appropriate to customers within Service Level Agreements. Test plans should be clearly documented and include instruction to notify involved parties of the occurrence of the test, disaster simulation and relocation as well as a defined timeline. Lastly, recovery plan review procedures should be included.

G. Applications and Data Criticality Analysis

Based upon system and configuration complexity and data importance resulting from the Kansas Health Information Network, Inc. Risk Analysis, the following applications are listed in order of importance, criticality and data sensitivity. System recovery and other contingency plan functions will be prioritized based upon this list.

2. The Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications.
3. The Director of Privacy and Data Compliance (DPDC) assures that solutions are implemented. This includes implementation of:
    - Data Back Up Plans.
    - Disaster Recovery Plans.
    - Emergency Mode Operations.
    - Testing and Revision.
    - Applications and Data Criticality Analysis.
4. Any and all related policies and procedures will be updated, including training materials. General awareness training for all workforce may include periodic "mock drills" on the identification and response for contingency operations, including those deemed most probable such as infection by malware (virus), cyber security issue, fire, water, and alarm incident procedures to assure workforce members are familiar with responsibilities to be performed during times of crisis. Lessons learned from ongoing incident handling activities and industry developments are incorporated into training materials.
    a. For workforce members assigned specific Incident Response Roles and Responsibilities, training includes dissemination of a copy of the Disaster Recovery Plan and specific Kansas Health Information Network, Inc. incident response and contingency processes related to data backup plan, disaster recovery, emergency mode operation, testing, revision, applications and data criticality analysis.
    b. Specific Incident Response training occurs within (90) days of assigned responsibilities and/or as a result of information system changes requiring retraining and then again annually as long as the responsibility is in place.
5. The Director of Privacy and Data Compliance (DPDC) will routinely monitor the Contingency Plan and related solutions by performing testing and process validation on a routine basis. When new requirements are added, revisions to evacuation plans and/or fall back procedures are addressed. Validation of the plan by testing is completed in order to continually assess the effectiveness of the Business Associate's ability to balance the confidentiality of PHI with its integrity and availability for use or disclosure so as not to negatively affect the process of health care.

Evaluation of the Privacy & Security of Protected Health Information	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 030
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.306, 164.308(a)(8)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer (CISO), Systems Support

Policy:

1. Kansas Health Information Network, Inc. will perform a routine and periodic annual technical and non-technical (operational) review of all of Kansas Health Information Network, Inc. policies and procedures. This initial evaluation will take into consideration initial Kansas Health Information Network, Inc. enterprise status and its resulting early interpretation of the Administrative Simplification Security components. This will be Kansas Health Information Network, Inc. benchmark evaluation.
2. The same review will subsequently be undertaken periodically and whenever environmental or operational changes affecting the protected health information secured by Kansas Health Information Network, Inc. occur. The benchmark evaluation will be used as the beginning of the second review.

Procedure:

1. Based upon workforce experience, objectivity and availability Kansas Health Information Network, Inc. may conduct its own internal assessment or evaluation of its privacy/cyber security/security compliance. Alternately, Kansas Health Information Network, Inc. may routinely or intermittently purchase the services of an external accreditation agency or professional association or other to undertake and complete the evaluation in the most objective manner taking into consideration Kansas Health Information Network, Inc. unique business needs.
2. Whether internal or external resources are utilized, the goal of evaluation is to conduct a review of Kansas Health Information Network, Inc. privacy/cyber security/security safeguards in order to demonstrate and document compliance with the HIPAA/HITECH requirements on an ongoing basis.
    2.1. The evaluation process consists of an objective review of Kansas Health Information Network, Inc. performance compared with its processes to secure protected health information, which were specifically set forth in the Kansas Health Information Network, Inc. policy and procedure documents. The actual measurement criteria may be unique to each policy and procedure, but functions to measure if the Business Associate's workforce performance is consistent with the processes defined in the policies and procedures. The unique acceptable level of measurement will be consistent with the results of the risk analysis. For example, if "Termination Procedures" have been implemented, the measurement criteria may be an annual review of workforce who have terminated in the past calendar year detailing the way the process occurred as compared to

the written policy and procedure defining how and when the actual access to PHI was withdrawn. The resulting time frames will be measured against those that have been predefined.

3. Evaluation should include the following at a minimum:
   3.1. Risk identified during initial or previous risk analysis.
   3.2. Risk Management Business Associates.
   3.3. Network Penetration of systems that contain electronic protected health information.
   3.4. Social Engineering of current workforce.
   3.5. Sanction and Termination Policy.
   3.6. Audit and Systems Activity Review Procedures.
4. Results will be formally communicated to the HIPAA Risk and Security Committee in a timely manner so that the following activities may begin:
   4.1. Identified challenge areas may be addressed.
   4.2. Subsequent mitigation activities can occur (SEE Change Control Policy and Procedure).
   4.3. Evaluation process may be repeated.

Device and Media Controls	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 031
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.310(d)(1) and 164.312(b)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC) and Chief Information Security Officer (CISO), Chief Operating Officer (COO)

Policy:

1. The Director of Privacy and Data Compliance (DPDC) and workforce members are s responsible for safeguarding the security and integrity of data stored on *electronic and physical media* whether in use during transit, storage, re-use, or after disposal. The purpose, scope responsibilities and compliance requirements are set forth within this policy.
2. Kansas Health Information Network, Inc. works to safeguard information contained on devices and media in two ways:
   2.1. Kansas Health Information Network, Inc. will maintain a comprehensive device and media control program for workforce members under its direct control.
   2.2. For the Independent Consultants (ICs) with which Kansas Health Information Network, Inc. contracts, written guidelines will be provided of Kansas Health Information Network, Inc. expectations for protecting PHI and company information when using technical devices and media.

Documentation of device and media controls for Kansas Health Information Network, Inc. includes:

- A description of the Kansas Health Information Network, Inc. personnel, or Independent Contractor, responsible to assure that protected health information in electronic format, as well as the hardware or electronic media on which it is stored, is properly destroyed and cannot be recreated.
- A description of the Kansas Health Information Network, Inc. personnel responsible or Independent Contractor, to assure that protected health information is removed from reusable media, such as USB devices, tapes, discs, Printers/Copiers (which have memory capability), CD-ROMs/diskettes before it is used to record new information.
- A description of the method used to record the movement and storage of hardware and electronic media into and out of Kansas Health Information Network, Inc.. This includes assigning an individual workforce member(s), or Independent Contractor, responsibility for documenting the receipt or removal of the hardware and electronic media so that the location of both are known at all times, and the action or event is traceable to that individual workforce member(s).
- As necessary and applicable, a description of the method used to create an exact retrieval copy of the data is made before the equipment holding the protected health information is moved.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to device and media controls. This ensures that the processes chosen to carry out safeguards relating to device and media controls are in accordance with the level of risk, priority, and importance assessed by Kansas Health Information Network, Inc..
2. The Director of Privacy and Data Compliance (DPDC) will create guidelines and a mechanism for device and media accountability, and to choose the Kansas Health Information Network, Inc. preferred technical solution and process to develop the procedures which function to reasonably safeguard Kansas Health Information Network, Inc. protected health information stored on devices and other media controls. The following factors should be considered:
   2.1. Reviewing the risk assessment results and related documentation.
   2.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
   2.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
   2.4. Thoroughly considering all areas defined below as "Implementation Considerations".
3. The Kansas Health Information Network, Inc. Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy.
4. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will ensure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process. This includes creating written documentation of Device and Media Control Guidelines for Independent Consultants to utilize.
5. The Director of Privacy and Data Compliance (DPDC) will additionally ensure that any and all related policies and procedures will be updated, including training materials.
6. To the extent that workforce functions are affected by the chosen solution, the Director of Privacy and Data Compliance (DPDC) will coordinate and ensure that the solution is implemented, and each affected member is trained. This includes training management personnel to ensure any and all devices or media containing sensitive Kansas Health Information Network, Inc. information or electronic protected health information is forwarded to the Privacy & Security Officer when no longer necessary for business use, or in preparation for reuse.
7. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out on a quarterly basis in order to continually assess the effectiveness of Kansas Health Information Network, Inc.'s ability to balance the confidentiality of the protected health information with its integrity and availability. This includes performance of routine, random audit checks of device and media controls in order to validate Kansas Health Information Network, Inc. compliance with this policy.

Implementation Considerations Relating to Device and Media Controls

Device and Media Accountability

1. Kansas Health Information Network, Inc. has instituted an asset inventory management process in order to record, at a workforce member level, the movement of hardware and electronic media into and out of Kansas Health Information Network, Inc. This means that every device or media control known To Kansas Health Information Network, Inc. to house electronic protected health information is:
   - Identified with a unique tracking number,
   - Labeled and encrypted according to its classification and criticality,

- Device description and disposition (including owner) of such device is documented in the asset inventory list.

This record keeping documentation clearly defines the transfer of responsibility by device or media that is received, maintained/monitored, re-used and/or, ultimately, disposed of by Kansas Health Information Network, Inc.. The asset inventory list is unique and does not unnecessarily duplicate other inventories. Kansas Health Information Network, Inc. will also provide written guidelines to its Independent Consultants on the suggested controls for device and media use. The following electronic data should be considered for inclusion in Kansas Health Information Network, Inc.'s Asset Inventory:

1.1. Company Devices, with hard drives, including and not limited to laptops, company mobile phones, and company tablets.

1.2. Data contained on removable, re-usable magnetic electronic data storage media, such as tapes, USB sticks, CD-ROMs.

1.3. Data contained on the hard drives of file servers, disk storage arrays, mainframe mini-or mid-range computers, or diagnostic equipment.

1.4. Data contained on the hard drives on personal computers that are transferred within one organization from one authorized to another, as well as those that are removed from Kansas Health Information Network, Inc. to be sold, recycled, or otherwise discarded.

1.5. Data contained on computing devices including laptops, desk computers, and any other related devices.

1.6. Digital and non-digital media.

Device and Media Control Form and Process

1. Kansas Health Information Network, Inc. uses the Device and Media Control form to record requests of disposal, sanitization, reuse or request of media, devices, or software modifications. Once received and processed, all information from the Device and Media Control Form is transferred into the Asset inventory. Forms shall include record of request and approval at both a business and information systems level. Specifically, the form shall include the following:

   1.1. Date and record of department requesting action.

   1.2. Description of the action requested which may include disposal, reuse, request, repair or transportation of device or media.

   1.3. Brief description of the sensitive information or electronic protected health information. contained on the device or media.

   1.4. Approval information

   1.5. Signature of workforce member to conduct process.

   1.6. Action taken that may include but not be limited to the following:

   - Sanitization or destruction method.
   - Existence of back-up copy and its disposition.
   - Labeling program, program changes.
   - Record of version numbers.
   - Maintenance or creation dates.
   - Information for production modules.

- Copies of previous versions.
- Current and control updates.
- Record of new user (if applicable).
- Record of repair via supplier or external service provider.

Maintenance and Service of Equipment

1. Authorized personnel conduct maintenance and service of equipment containing sensitive information based on supplier-recommended maintenance intervals and in accordance with applicable insurance policies.
2. Sensitive information/PHI is removed from equipment prior to maintenance unless explicitly allowed by the Privacy Security Officer.
3. Appropriate escort and/or limited and supervised access is in place while outside personnel conduct maintenance and/or service on-site based on specific technical competence.
4. Remote diagnostic activities and non-local maintenance must be pre-approved in writing and monitored by the Privacy Security Officer.
5. After maintenance, security controls are verified and rechecked to assure data integrity.
6. Records of maintenance are maintained.
7. Spare parts if needed to allow for the Recovery Time Objective defined within the Contingency Plan to be met are stored in accordance with this policy.

Device and Media Reuse

1. The Kansas Health Information Network, Inc. Chief Operating Officer (COO)is responsible to assure that all devices and media equipment including storage media/surplus equipment, and other hardware containing sensitive information or electronic protected health information shall be safeguarded while in storage and sanitized prior to reuse. Sanitization methods may include:
    1.1. Procedures to clear sensitive data from discarded and transferred equipment or media.
    1.2. Sanitization or factor reset of company devices.
    1.3. Degaussing or complete overwriting of electronic media.
    1.4. Other procedures to clear sensitive data from discarded and transferred equipment or media.
2. A final attempt to access the sensitive information will be made to assure sanitization was completed prior to the time that the device or media was forwarded to the next user.
3. Method of sanitization and record of new user assignment, along with the date and time and signature of person who conducted the process will be logged in the asset inventory list in accordance with Kansas Health Information Network, Inc. policy.

Device and Media Disposal

1. The Kansas Health Information Network, Inc. COO or his/her designee, is responsible for retrieval and proper disposal of all devices and media containing sensitive Kansas Health Information Network, Inc. data and/or electronic protected health information. All devices and media equipment including storage media in personal computers and other hardware containing sensitive information or electronic protected health information shall be sanitized prior to disposal. Sanitization and destruction methods may include but are not limited to the processes listed below and should be assigned in accordance with the sensitivity of the information to be disposed:

1.1. Burning.

1.2. Mulching or pulping.

1.3. Shredding or disintegrating.

1.4. Degaussing or complete overwriting of electronic media.

1.5. Other procedures to clear sensitive data from discarded and transferred equipment or media.

2. A final attempt to access the sensitive information will be made to assure destruction was complete.
3. Method of destruction used, along with the date and time and signature of person who conducted the process will be logged either manually or automatically in the inventory library in accordance with Kansas Health Information Network, Inc. policy.

Technical Access Controls and Other Related Safeguards	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 032
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.312(c)(1)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Chief Information Security Officer, Systems support

Policy:

1. Kansas Health Information Network, Inc. protects all electronic PHI via multiple access control and other technical mechanisms and systems. Use of multiple access controls allows Kansas Health Information Network, Inc. a layered approach to security. This provides a greater security level as more than a single point of failure must occur before electronic PHI can be accessed inappropriately.
2. Access Profiles

   Kansas Health Information Network, Inc. maintains RBA-C profiles to specify which PHI may be used by workforce members in each job class. These profiles specify the level of access to protected health information.

   Kansas Health Information Network, Inc. assigns a unique user identification number to all workforce members who access and use electronic PHI in performance of their job. The Systems support resource creates, assigns and revokes user identification numbers and names. Kansas Health Information Network, Inc. holds all workforce members accountable for the actions using or disclosing electronic protected health information under their unique user identification number, name and via multi-factor authentication and the Acceptable Use Agreement.
3. Emergency Access

   Kansas Health Information Network, Inc. must always be prepared to balance the confidentiality of electronic PHI with its availability, even during an emergency. Therefore, Kansas Health Information Network, Inc. has developed an emergency access policy and procedure:

   - For obtaining necessary electronic PHI using an emergency access device, such as a key, password, code or digital certificate.
   - For triggering use of the Emergency Mode of Operation Plan, which is stored securely off-site.
4. Automatic Log Out or Log Off

   Kansas Health Information Network, Inc. (enterprise wide) employs the use of automatic log-off after 30 minutes of inactivity.
5. Encryption and Decryption

   Kansas Health Information Network, Inc. utilizes encryption and decryption mechanisms as a form of control for electronic PHI.
6. Other technical and physical controls are in place to collectively assure PHI is safeguarded. These include but are not limited to technical controls ensuring the security of the information contained within networks, the availability of the network services and the information services using the network as well as the protection of the connected services from unauthorized access.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to all areas of access controls. This assures that the processes chosen to carry out access control are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc..
2. The Director of Privacy and Data Compliance (DPDC) is responsible to choose the Kansas Health Information Network, Inc. preferred combination of process and technical solution(s) to develop the procedures which function to reasonably safeguard PHI and make up technical access controls, other technical controls and physical controls by considering the factors listed below:
   2.1 Reviewing the risk assessment results and related documentation.
   2.2 Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
   2.3 Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
   2.4 Thoroughly considering all areas defined in the procedure as "Implementation Considerations.
3. The Director of Privacy and Data Compliance (DPDC) assigns managers/owners for application systems who are responsible for strict security control of the support environment or related project and are responsible to check and approve all proposed systems changes to assure they do not compromise the security of the system, operating environment or related data.
4. Connections from Kansas Health Information Network, Inc.'s information system to other information systems residing outside of Kansas Health Information Network, Inc. occur only in accordance with formal interconnection security agreements. These include details about the connections, the interface characteristics, nature of the information communicated and security requirements; employ a deny all, permit by exception policy and apply a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (servers, workstations), except for those explicitly allowed.

Implementation Considerations Relating to Access Control

RBA-C Profiles

Kansas Health Information Network, Inc. maintains RBA-C profiles to specify which PHI may be used by workforce members in each job class.

- Redundant user IDs are not issued to other users and all users are uniquely identified and authenticated for both local and remote access to information systems.
- Users who perform privileged functions (e.g., system administration) use separate accounts when performing those privileged functions.
- Access for individuals responsible for administering access controls is limited to the minimum necessary based upon each user's role and responsibilities and these individuals cannot access audit functions related to these controls.
- Shared/group and generic user IDs are only used in exceptional circumstances where there is a clear business benefit, when user functions do not need to be traced, additional accountability controls are implemented, and after approval by management.
- Unique IDs are used to trace activities to the responsible individual and are required for all types of organizational and non-organizational users. Non-organizational users (all information system users other than organizational users, such as clients/customers, contractors, or foreign nationals), or processes acting on behalf of non-organizational users, determined to need access to

information residing on Kansas Health Information Network, Inc.'s information systems, are uniquely identified and authenticated.

- All file system access that is not explicitly required is disabled and only authorized users are permitted access to the information expressly required based on their job function. Unnecessary and default system accounts are disabled, removed or otherwise secured (passwords changed and/or privileges reduced.)
- Users are allowed to connect to the internal network based on a restricted deny-by-default and allow-by-exception policy at routine interfaces in accordance with the access control policy and based on business requirements.
- Physical or logical access is only given to suppliers for support purposes, when necessary, with management approval, and such access is monitored.

Electronic Signatures

If used, Kansas Health Information Network, Inc. requires that electronic signatures, unique to one individual, cannot be reused by, or reassigned to, anyone else.

- Kansas Health Information Network, Inc. ensures individuals are held accountable and responsible for actions initiated under their electronic signatures, to help deter record and signature falsification.
- Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners.
- Electronic signatures and handwritten signatures executed to electronic records are linked to their respective electronic records.
- Signed electronic records contain information associated with the signing in human-readable format.

Unique User Identification and Authentication

This assignment of unique user identification allows for systems to identify each user and hold individuals accountable for their actions. This assignment is the entry point for many other technical safeguards including audit controls, integrity, and person or entity authentication.

- Multi-factor authentication methods are used for all workforce members.
- When tokens are provided for multi-factor authentication, in-person verification is required prior to granting access.
- Help desk support requires user identification for any transaction that has information security implications.
- When PKI-based authentication is used, certificates are validated by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; enforcing access to the corresponding private key; mapping the identity to the corresponding account of the individual / group; and using a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network.
- Replay-resistant authentication mechanisms are used such as nonce, one-time passwords, or time stamps to secure network access for privileged accounts; and, for hardware token-based authentication, employing mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline.

Emergency Access Controls

- Kansas Health Information Network, Inc. has identified and prioritized the probability of various kinds of emergencies.
- Kansas Health Information Network, Inc. has considered the amount of maximum outage that can sustained while continuing to provide electronically controlled access to PHI.
- Kansas Health Information Network, Inc. has defined when other Contingency Planning and Emergency Mode Operations should be invoked.

Kansas Health Information Network, Inc. has established temporary access authorizations (emergency access codes to be used during time of crisis) necessary during an emergency. These are maintained by the helpdesk and documented in a standard manner and securely maintained.

Kansas Health Information Network, Inc. uses system configuration and automatic log off/ log out controls to insure appropriate access to electronic PHI.

- Session screens are paused via a time-out system (e.g. a screen saver) after a predefined amount of minutes of inactivity and network sessions are closed after 30 minutes of inactivity.
- A time-out system (e.g. a screen saver) pauses the session screen and closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.
- Computer login banners are displayed outlining the terms and conditions of access and are accepted before access is granted.

Encryption Controls

Kansas Health Information Network, Inc. uses encryption and decryption as a form of control for electronic PHI at rest.

Other Technical Control Considerations and Mechanisms

- Formal management of all equipment on the network, including equipment in user areas is in place. See Device and Media Controls and Integrity Policies and Procedures.
- The initiation of an event is separated from its authorization in order to reduce possible collusion.
- Ports, similar applications and services installed on a network or computer system which are not required for business purposes/functions are removed or disabled.
- Bring your own device (BYOD) and/or company-owned devices are configured to require an automatic lockout screen, and the requirement is enforced through technical controls.

- The organization's system clocks are synchronized to an agreed, authoritative real-time standard (e.g., daylight savings time) and synchronized daily as well as at system boot.
    - Kansas Health Information Network, Inc. prevents program execution in accordance with the list of unauthorized (blacklisted) software programs and rules authorizing the terms and conditions of software program usage. Blacklisted or unauthorized software on the information system, including servers, workstations and laptops, employ an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (blacklisted) software on the information system, and reviews and updates the list of unauthorized (blacklisted) software periodically but no less than annually. Automated controls (e.g. browser settings) are in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).

Technical Network, Security Gateway and Routing Controls

- Routing controls are implemented through security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and third-party networks).
- The network is physically and logically segmented via a defined security perimeter and graduated set of technical controls including subnetworks for publicly accessible system components and traffic controlled based on functionality and classification of data and systems based on a risk assessment and their respective security requirements.
- Kansas Health Information Network, Inc. uses at least two DNS servers located on different subnets, which are geographically separated and perform different roles (internal and external) to eliminate single points of failure and enhance redundancy.
- Authoritative DNS servers are segregated into internal and external roles.
- Firewalls and security gateways are in alignment with security policies (including but not limited to Access Control) for traffic control and configured to block unauthorized access, filter traffic between domains and used to maintain appropriate segregation between internal wired/wireless and external network segments (Internet and/or telecommunication service manager interface), include DMZs and enforce access control for each respective domain. Exceptions for traffic flow must be documented with business justification, duration of the exception must be temporary and subject to be reviewed at least annually; traffic flow policy exceptions are removed when no longer supported by an explicit mission/business need.
- Inbound and outbound traffic is restricted to the minimum necessary by firewalls. Firewall configurations restrict connections between untrusted networks and system components within the covered environment or to restrict inbound and outbound traffic to that which is necessary for the covered environment. Any changes to the firewall configuration are updated in the network diagram. Outbound traffic is forced to the Internet via an authenticated proxy service on the enterprise perimeter.
- A formal and current Technical Network Diagram which includes wireless networks is in place and is updated at least every six months or more frequently if there are changes.
- By formal agreement or other documentation, the following policy is set forth which includes either of the following: i) allow-all, deny -by-exception or ii) deny-all, permit-by-exception (which is preferred) to allow specific information systems to connect to external information systems.
- Access rights from one application to another are technically controlled. Outputs from application systems with PHI are limited to the minimum amount necessary and only sent to authorized locations/terminals.
- Remote access connections between external parties And Kansas Health Information Network, Inc. are encrypted. Access by external parties is granted for a limited duration and only to the minimum amount necessary based on job functions. Access for external information assets (where Kansas Health Information Network, Inc. has no control) is based on clearly defined conditions and terms. Remote devices establishing a non-remote connection are not allowed to communicate with remote (or external) resources.
- All network connections and firewall, router and switch configuration changes are tested and formally approved prior to implementation. Deviations from the standard or updates are documented in accordance with the Change Control and Systems Development Life Cycle Policies and documents.
- Requires for network routing are in alignment with the access control policy including positive source and destination checking mechanisms (such as firewall validation of source/destination addresses and hiding of internal directory services or IP addresses). Network perimeters are designed so that all outgoing network traffic to the Internet must first pass through at least one

application layer filtering proxy server. The Proxy server supports decrypting network traffic, blocking specific URLs, domain names, logging of individual TCP sessions and IP addresses to implement a blacklist and use of whitelists of allowed sites accessed via proxy while blocking all other sites.

- Remote activation of collaborative computing devices is prohibited via the information system including an explicit indication of use to users who are physically present at the device.
- The organization tests and approves all network connections and firewall, router, and switch configuration changes prior to implementation. Any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system. All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network devices (like firewalls and IPS) are documented, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need, and processed in accordance with formal Change Control protocols.
- Installation checklists and vulnerability scans are used to validate the configuration of servers, workstations, devices, and appliances, and ensure the configuration meets minimum standards.
- The organization employs automated mechanisms to (i) centrally manage, apply, and verify configuration settings; (ii) respond to unauthorized changes to network and system security-related configuration settings; and, (iii) enforce access restrictions and auditing of the enforcement actions.
- Unless the risk is identified and accepted by the data owner, sensitive systems are isolated (physically or logically) from non-sensitive applications/systems.
- Shared system resources (e.g., registers, main memory, secondary storage) are released back to the system, protected from disclosure to other systems/applications/users, and users cannot intentionally or unintentionally access information remnants.

Wireless Networks and Mobile Computing Controls

- An inventory of authorized wireless access points, including a documented business justification to support unauthorized WAP identification and response is in place.
- Wireless Access Points are placed in secure locations and are configured with strong encryption (AS WPS2 at a minimum).
- Vendor defaults for wireless access points are not used but are changed prior to authorization/implementation of the access point.
- Routine (at least quarterly) scans for unauthorized wireless access points are conducted and mitigation is taken as necessary should inappropriate access be discovered. Ongoing monitoring for all unauthorized and authorized wireless access to the information system takes place. The installation of wireless access points (WAPs) is prohibited unless specifically authorized in writing by the Chief Information Security Officer (CISO).
- Mobile computing devices are protected by access controls, connection requirements, usage restrictions, encryption, virus protection, firewalls, secure configurations, and physical protections at all times. Additionally, remote wipe functionality is in place for any mobile devices connecting to networks or storing/accessing PHI and/or organizational information.
- The organization monitors for unauthorized connections of mobile devices.
- Circumvention of built-in security controls for mobile devices such as jailbreaking, or rooting are prohibited.

- A list of approved and allowable application stores for mobile device accessing or storing organizational or cloud service provider managed data exists. The use of unapproved application stores is prohibited.
- Formally defined usage restrictions and implementation guidance for VoIP including the authorization and monitoring of service are in place.
- Networks are segregated from production-level networks when migrating physical services, applications or data to virtualized servers. Secure and encrypted communication channels are used.

Physical Facility Controls-Kansas Health Information Network, Inc. is a virtual company. These controls are in documented if at some point Kansas Health Information Network, Inc. establishes a physical location.

- Physical protections limit access to network equipment.
- Access to diagnostic and configuration ports include controls via a key lock and supporting procedures to control physical access to the port.
- A list of individuals authorized to physically access the facility where information systems reside is developed, approved and maintained. Authorization includes review of credentials for facility access, ongoing review of access lists via period review (at least quarterly) as well as removal/termination as appropriate.
- Facilities where information systems reside restrict physical access authorization to defined entrance/exit points, maintain physical access audit logs and other security safeguards as necessary for areas designated accessible by the public.
- Modifications and repairs to the physical components of the facility related to security such as but not limited to walls, doors, locks, hardware are documented and retained in accordance with the retention policy.

  Other technical mechanisms used to help protect and limit access to Kansas Health Information Network, Inc. electronic PHI may include:

  Network firewalls, Secured gateways and proxies, Call-back systems, Network segmentation, Intrusion prevention systems, and Anti-virus systems and proper OS patch maintenance.

5. The Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications.
6. The Director of Privacy and Data Compliance (DPDC) ensures the solution is implemented in a timely manner and that all affected policies and procedures are updated accordingly. Any necessary training will also be carried out. Training may include "log-out" curriculum so that a user is familiar with automatic log off/out policy due to inactivity of system use within a certain and specific amount of time. It may also include planning and coordinating of routine drills and global training in order to ensure that Kansas Health Information Network, Inc. is prepared to respond during an emergency.
7. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out routinely in order to continually assess the effectiveness of Kansas Health Information Network, Inc.'s ability to balance the confidentiality of the PHI with its integrity and availability. This routine monitoring includes review of all technical and non-technical solutions to assure they are maintained in optimal order to allow for Kansas Health Information Network, Inc. to be continually prepared to respond in the event of an emergency.

Change Control	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 033
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.312(c)(1)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Systems support, Operations/Business

Policy:

1. The ultimate goal of the Kansas Health Information Network, Inc. Change Control Program is to assure a consistent method is followed to support the optimal functioning of the Management Information System and all critical components, even though ongoing patches, upgrades and other changes must be applied. A formal Change Control process reduces or eliminates disruptions, minimizes potential corruption and maintains acceptable levels of service during the implementation of changes. This occurs by monitoring and managing the:
   - 1.1 Prioritization of changes.
   - 1.2 Frequency of changes.
   - 1.3 Impact of Changes on Processes.
   - 1.4 Length of time required to implement changes.
   - 1.5 Changes resulting in problems.
   - 1.6 Concurrent Changes.
2. The Director of Privacy and Data Compliance (DPDC) has developed a formal Change Control Process which includes definition of scope, roles and responsibilities, management commitment, coordination and compliance to accomplish the following:
   - 2.1 Set forth a formal method to control, document, and archive all changes to information assets including systems, networks, and network services.
   - 2.2 Create a central workflow process for the consistent management, coordination, control and documentation of all change management functions affecting systems and software.
   - 2.3 Create an inventory for all information systems and current upgrade status.
   - 2.4 Develops, documents, and maintains, under configuration control, a current baseline configuration of the information system, and reviews and updates the baseline as required. Configures system security parameters to prevent misuse.
   - 2.5 Include testing and validation components to assure security features and controls are not altered or compromised as a result of a hardware or software change.
   - 2.6 Assure that Change Control meets vendor contractual obligations (as applicable). This means that vendor supplied software used in operational systems is maintained at a level supported by the

supplier, and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application.

2.7 Aligns Change Control process with configuration management plan program to ensure formal management of configuration settings for information technology products employed within the information system using the latest security configuration baselines; (ii) identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements; and, (iii) monitors and controls changes to the configuration settings in accordance with Kansas Health Information Network, Inc.'s policies and procedures.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to technical controls and configuration management. This assures that the processes chosen to implement Change Control are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc. Further the security controls selected reflect the business value of the information assets involved and the potential damage that might result from a failure or absence of security. The following factors should be considered:

   1.1 Review of the risk assessment results and related documentation.

   1.2 Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

   1.3 Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.

   1.4 Thoroughly considering all areas defined in the procedure as "Implementation Considerations".

   Implementation Considerations Relating to Change Control.

   Suggested Elements of the formal Change Management Process:

   - Documentation of the Change Request.
   - Assessment of the Change (by both Technical and Business/Operations SMEs).
   - Approval by Management of the Change.
   - Detailed documentation as necessary and in accordance with methodology chosen.
   - Development (as applicable).
   - Testing – with applicable approval.
   - Implementation – with applicable approval.
   - Reporting.

   Technical Recommendations:

   - Installation checklists and vulnerability scans are used to validate the configuration of servers, workstations, devices and appliances and ensure the configuration meets minimum standards. Minimum hardened configuration standards are in place for all system and network components of the system to assure such systems are configured with only necessary and secure services, ports and protocols enabled.

- Rules for the migration of software from development to operational status are defined and documented in a formal Systems Development Life Cycle document prepared by Kansas Health Information Network, Inc. hosting the affected application(s), including that development, test, and operational systems must be separated (physically or virtually) to reduce the risks of unauthorized access or changes to the operational system. Developers must identify and document the functions, ports, protocols and services early in the systems development life cycle. The Systems Development Life Cycle (SDLC) must include detailed Information System Specifications which include security requirements, whether manual or automated to be applied as software packages are evaluated, whether developed in-house or purchased. Data integrity/validation checks for information inputs for accuracy, validity, completeness and authenticity are a component of the SDLC as close to the point of origin as possible.
- A prioritization process is in place to determine which patches are applied across operating systems. Patches installed on production systems are also applied to the disaster recovery environment in a timely manner.
- A rollback strategy is in place before changes are implemented, and an audit log is maintained of all updates to operational program libraries.
- Fallback procedures are defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events. When additional functionality is supplied and causes a security issue, the functionality is disabled or mitigated through the use of additional controls.
- Automated updates are not used on critical systems.
- Workforce who manage application systems are also responsible for the strict control (security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.
- Should Kansas Health Information Network, Inc. develop its own applications, these are based upon secure coding guidelines to prevent common vulnerabilities. Additionally, explicit error checking is performed and documented for all input, include the data type, size, acceptable formats and ranges.
- Only authorized administrators are allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.
- Patches, applications and operating systems are tested for usability, security and impact prior to production. Operational systems only hold approved programs or executable code.
- Technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging support the operating system as part of its baseline.
- Mobile device changes to operating systems, patch levels, and/or applications are handled via formal change management process for devices that connect to corporate networks or store and access company information.
- Should technical code development be outsourced, security change control procedures included in the respective contract and specifically require the developer to track security flaws and flaw resolution within the system, component, or service and appropriately report findings.

- If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, Kansas Health Information Network, Inc. must show evidence of a formal migration plan approved by management to replace the system or system components.
- Should the security functionality in a proposed product not meet the specific requirement, the associated controls and risks are re-evaluated prior to purchasing the product.

2. The Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This includes a separate review of all Change Requests nearing Implementation to allow for constant prioritization of changes released to Production.
3. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will assure it is implemented in a timely manner and that all affected policies and procedures are updated and training on such occurs as necessary.
4. Change Records reference the configuration management plan to maintain control of all implemented software and its system documentation, and archives prior versions of implemented software and associated system documentation.
5. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the PHI with its integrity and availability. The monitoring includes:

   5.1 Completion of thorough investigation and mitigation activities in response to Change Control

   5.2 Routine review of new technologies in order to more specifically define, capture, and retain Change Control workflow and reporting documentation.

Audit Controls	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 034
Section: ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.312(b)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Systems support

Policy:

The audit trail process is an operational process that serves to consolidate all audit mechanisms for the Business Associate. It provides a means to detect security breaches and intentional alterations as well as a method to identify errors or duplicate information. This includes administrative, physical and technical components such as the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI. The audit trail includes all system activities (create, read, update and delete) and is used to identify irregularities or anomalies which may indicate system compromise or malfunction and facilitate the optimal, resilient and secure state of the system.

Kansas Health Information Network, Inc. has defined its level of audit trail monitoring by carefully considering the level of and types of information to be recorded, the capability of the automated information system and all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.

Procedure:

The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to audit controls. This assures that the processes chosen to implement audit controls are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc.

1. The Director of Privacy and Data Compliance (DPDC) is responsible to determine what information is reviewed, how it is captured, and when it is suspicious in order to choose the Kansas Health Information Network, Inc. preferred combination of process and technical solution(s) to develop the procedures which function to reasonably safeguard Kansas Health Information Network, Inc. PHI. The Director of Privacy and Data Compliance (DPDC) must also make up audit controls by considering the following factors:

    1.1. Reviewing the risk assessment results and related documentation.

    1.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

    1.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.

    1.4. Thoroughly considering all areas defined in the procedure as “Implementation Considerations”.

    Implementation Considerations Relating to Audit Control Criteria

    Audit Trail Definition

The data selected for audit trail is captured on the Kansas Health Information Network, Inc. SLA spreadsheet and is reviewed by the security team on a bi-monthly basis. It is tracked in chronological form. It is created immediately concurrent (real time) as the user conducts the action of access and is inclusive from initial access to completion of action. The integration of intrusion detection into workflow processes including the use of automatic alerts based on defined triggers such as malicious code and/or potential intrusions is incorporated.

- It may include creation of records to log.
- Who saw what information (unique user identification and data source; administrator activities including operating logs).
- How the event was initiated (command, program).
- Key Event Monitoring - Type of event and its result (what data was compromised with unique data subject ID). Examples may be:
    - File integrity monitoring (inbound and outbound communications accessed),
    - Command or program used to initiate the event and source/destination addressed
    - The success/failure of data accessed,
    - System security configuration changes,
    - Utility or privileged use,
    - Alarms raised, de-activation or activation of protection systems like IDS/IPS, activation/de-activation of authentication mechanisms,
    - Creation or deletion of system level objects,
    - Cybersecurity events should be noted as well.
- At what time and date,
- On which individual and reason for access (this is the nature of activity including change, review, update or delete),
- On which system did the event take place, include hardware, software and/or procedural mechanisms.

For Privileged Users (Operators and Administrators)

Audit trails include the success/failure of the event, time of the event, the account involved, the process involved, and the additional information related to the event.

Authorized and/or unauthorized access attempts along with attempts to deactivate accounts, system alerts or failures should be included.

For Messages Sent and Received

Audit trails include the date, time, origin and destination of the message, but not the content.

Audit Trail Mechanisms

The mechanism used to capture audit trail information allows for the collection and aggregation of information across multiple sources to support audit reduction and report generation. Automated tools are used to routinely identify, organize and prioritize reporting of suspicious records such as:

- Intrusion detection system (IDS)/ information protection system (IPS) managed outside of the control of the system with monitoring of network administrator activity,
- Use of a Security Information and Event Management (SIME) tool which facilitates the aggregation of information across multiple systems with configured profiles allowing for more efficient identification of issues,

- Unauthorized remote connections are monitored and reviewed at least quarterly with appropriate action taken should unauthorized connections be discovered.
- Use of automated warning messages that appear prior to a user accessing certain sensitive information. The message warns about the performance of routine audit and Kansas Health Information Network, Inc. responses for inappropriate activity.

Audit Trail Documentation and Retention

Kansas Health Information Network, Inc. has defined the process to collect and maintain audit trails, logs and file access reports in exact and retrievable copy form in a secure manner. Detailed audit records must be immediately available for retrieval for 90 days; older records should be archived for at least one full year. Records relating to compliance with HIPAA should be retained for at least six years. Process and mechanism may include system prevention of overwriting and unauthorized modification of audit trails (controlled access) assigned only to workforce responsible to monitor audit log.

Workforce Accountability

Kansas Health Information Network, Inc. has designated workforce responsibility to perform routine or requested review of logs (include frequency, extent, and nature of reviews, required documentation and credentials necessary for workforce assigned to conduct reviews). These include the following items.

Include definition of criteria to perform routine review whenever certain occurrences trigger one.

- Define controls to limit the opportunity that the actual audit trails may be modified.
- Implement mechanism(s) to capture and track security incident tracking reports.
- Define the level of management authority necessary for clearing investigation when inappropriate activity is suspected.

2. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will assure it is implemented in a timely manner and that all affected policies and procedures are updated and training on such occurs as necessary. This includes:

   2.1. The implementation of automatic alert generation so that technical workforce can analyze and investigate suspicious activity or potential violations and

   2.2. Periodic testing of monitoring, and detection processes, mitigation of any findings and ongoing improvement of process.

3. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the PHI with its integrity and availability. The monitoring includes:

   3.1. Completion of thorough investigation and mitigation activities in response to audit trail results.

   3.2. Routine review of new technologies in order to more specifically define, capture, and retain security incident tracking reports and audit trail information.

Integrity	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 035
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.312(e)(1)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC)

Policy:

1. Kansas Health Information Network, Inc.'s ability to preserve the integrity of the electronic PHI in its possession is directly dependent upon the successful implementation of a combination of policy and technical solution(s). The combination includes:
    1.1. Policies and procedures to protect electronic PHI from improper alteration or destruction and keep it consistent with its source.
    1.2. Electronic mechanisms to corroborate that the electronic PHI has not been altered or destroyed in an unauthorized manner.

Procedure:

The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to integrity controls. This ensures that the processes chosen to provide integrity controls are in accordance with the level of risk, priority, and importance assessed by Kansas Health Information Network, Inc..

1. The Director of Privacy and Data Compliance (DPDC) is responsible to choose the Kansas Health Information Network, Inc. preferred combination of technical solution and process to develop the procedures which function to reasonably safeguard Kansas Health Information Network, Inc. PHI and make up integrity controls. The following factors are to be considered:
    1.1. Reviewing the risk assessment results and related documentation.
    1.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
    1.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
    1.4. Thoroughly considering all areas defined in the procedure as "Implementation Considerations".
2. The Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution (s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc.'s retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications and Implementation Considerations as listed below.
3. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will ensure the solution is implemented in a timely manner, and that any affected policies and procedures are updated, and workforce trained as necessary.

4. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out in order to continually assess the effectiveness of Kansas Health Information Network, Inc.'s ability to balance the confidentiality of the protected health information with its integrity and availability.

Implementation Considerations Relating to Integrity Controls

Data Authentication Controls

Authentication of electronic PHI is the technical process of corroborating or validating that data has not been altered or destroyed in an unauthorized manner. The organization employs integrity verification tools to detect unauthorized, security-relevant configuration changes to software and information.

- Database integrity – integrity checking, and data recover features such as check sums, hashes, data duplication, transaction logging and error-correcting memory.
- Message integrity – transmitting electronic PHI from one place to another uses data integrity features including check sums, message authentication codes and other transport-level data integrity protocols, as well as higher-level mechanisms such as digital signatures.
- Procedure integrity – based on the level of risk it may be necessary to use redundant systems to store electronic PHI such as disc systems that are mirrored or configured in a RAID (redundant array of independent disks), SANS (Storage Area Network), duplicate power systems and appropriate power conditioning and cooling systems. Regular preventive maintenance must be performed.
- Virtual Machine images integrity – Integrity is ensured at all types by (i) logging and raising an alert for any changes made to virtual machine images, and (ii) making available to the business owner(s) and/or customer(s) through electronic methods (e.g., portals or alerts) the results of a change or move and the subsequent validation of the image's integrity.

Controls for Data While in Transit

Integrity controls focused on electronic PHI while in transit are designed to assure data is not improperly modified until it reaches its appropriate destination or is disposed of. Technical solutions that assist in preserving data while in transit may include

- Use of firewalls.
- Cryptography- Strong cryptography protocols are used to safeguard PHI during transmission over less trusted/open public networks.
- Other authentication devices such as use of multi-factor authentication.
- Also consider Transmission Security and use of encryption.
- Technical compliance checks are used to help support trust when supporting technical interoperability.

Password Security: Controls for Data While at Rest

The DPDC will assure the following are implemented:

- All systems-level passwords (e.g., root, enable, NT admin, application administration accounts) are changed on a periodic basis, which complies with the most recent guidance on security best practices for passwords and all user-level passwords (e.g., e-mail, web, desktop computer) are changed on periodic basis.
- User identities are verified prior to password resets. Users must acknowledge receipt of passwords by signing the Acceptable Use Agreement, acknowledging their responsibility to keep passwords confidential.

- Passwords must not be inserted into e-mail messages, scripts or databases or stored in any other electronic form unless encrypted.
- The DPDC will maintain a list of commonly used, expected or compromised passwords which is reviewed/revised at least every six months or when passwords are suspected to have been compromised.
- Passwords must meet three of four complexity requirements:
    - Contain at least 8 characters (and may include up to 64 characters to support the use of long passwords and phrases),
    - Contain both uppercase and lowercase characters,
    - Include numbers, digits,
    - Special characters,
- Passwords must:
    - Be easy to remember,
    - Not contain single words in any language, slang, dialect or jargon,
    - Be unique and not guessable,
    - Not be displayed when entered or included in automated log-on processes,
    - Not be communicated or disseminated via third parties or clear text (unprotected) electronic mail messaging,
    - Not be based on personal information such as names of family, places, etc.,
    - Only be transmitted if cryptographically protected (encrypted),
    - Be stored/maintained using an approved hash algorithm and encrypted,

The following considerations should also be made when using passwords in order to preserve integrity of data:

- Use of multi-factor authentication technology in combination with passwords.
- Use of encryption and decryption to further safeguard data at rest.
- Passwords are to be changed for default system accounts; upon any potential compromise; at first logon after a temporary password has been issued; and requires immediate selection of a new password upon account recovery.
- If using electronic signatures, identification codes are used in conjunction with passwords. If not based on the use of biometrics, employ at least two distinct identification components.
- If applicable to mobile devices, specific password technical controls should include Bring Your Own Device usage and not allow the changing of PIN lengths/passwords and authentication requirements.

Software Controls

Systems that do not have adequate authorization mechanisms are never to be used to store or transmit electronic PHI. The design of software used by Kansas Health Information Network, Inc. should be evaluated for its ability to:

- Protect against alteration or modification.
- Record missing or critical information.
- Control simultaneous updates.

Formal Change Control

A formal consistent method to identify, prioritize, record and track all systems changes through to end of life cycling is in place. See Formal Change Control Policy and Procedure.

Workforce Protocols

Kansas Health Information Network, Inc.'s ability to preserve integrity of data is dependent upon the successful implementation and workforce compliance with all other Security policies.

Authentication of Person or Entity	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 036
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.310(d)(1) and 164.312(d)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC)

Policy:

Kansas Health Information Network, Inc. uses a combination of operational policies and technological solutions to validate or authenticate that a person or entity attempting access to electronic protected health information in Kansas Health Information Network, Inc. possession is the one claimed to be. Corroboration can be made from a compilation of:

- Something workforce member/entity has (card, token, or key).
- Something workforce member/entity knows (password, personal identification number).
- Something related to who the workforce member/entity is (signature, iris, fingerprint).
- Something where workforce member/entity is located (network address, terminal connected by hardwired line).

Procedure:

The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to the authentication of a person or entity. This assures that the processes chosen to carry out the combination of policy and technical solutions for person or entity authentication are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc..

1. The Director of Privacy and Data Compliance (DPDC) is responsible to choose the Kansas Health Information Network, Inc. preferred combination of process and technical solution(s) to develop the procedures to authentication person or entity by considering the following factors:
   1.1. Reviewing the risk assessment results and related documentation.
   1.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
   1.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
   1.4. Thoroughly considering all areas defined in the procedure as “Implementation Considerations”.

Implementation Considerations Relating to Person or Entity Authentication

Kansas Health Information Network, Inc. Authentication of a person or entity is the process of corroborating or validating through the use of information that the person or entity is the one claimed. Technical Solutions supporting such corroboration or validation may include:

Password/Passphrase Configuration and Usage Controls

- Configuration of system for password encryption.
- Passwords must be at least 8 characters and meet three of four complexity requirements (e.g., upper- and lower-case characters, numbers, special characters) or otherwise has an equivalent strength (entropy).
- Password deactivation controls.
- Single session passwords.
- Configuration of user identification numbers consistent across organizations.

Additional Safeguard Controls

- Access Controls (establishment, modification, and termination).
- Audit Trails.
- Multi-Factor Authentication such as Duo, Kerberos and CHAP (for external connections to the network required prior to establishing a connection that includes at minimum, use shared information (i.e. MAC or IP address) and access control lists to control remote network access).
- Biometric authentication- physical features, hand, fingerprint, voice.
- Cryptographic integrity mechanisms (node authentication to authentication groups of remote users when connected to a secure shared computer facility).
- Deactivation of remote access by vendors and business partners when not in use.
- Device authentication, including wireless networks using either a (i) shared known information solution or (ii) an organizational authentication solution, the exact selection and strength of which is dependent on the system categorization of the information system.
- Digital systems, digital signatures.
- Encrypted authentication protocols, Encryption technologies (secret or public key).
- Magnetic swipe cards with PIN.
- Separation of an event from its authorization to reduce the possibility of collusion.
- Separation of Duties limits the risk of unintentional or unauthorized modification of systems/data:
    - Incompatible duties are separated across multiple users in order to minimize the potential for fraud or misuse.
    - No single person is able to access, change information systems/data without detection.
    - Duties requiring separation of duties are defined and documented and used to configure systems access authorization processes. Related job descriptions include separation of duties across multiple users.
- Smart card tokens, soft tokens.
- Technical Access Controls to allow all (deny by exception) or deny-all, permit by exception (preferred) protocols for systems connections.
- Token-based authentication systems.

- Workforce incentives to reduce sharing of information.
- Workforce sanctions to reduce sharing of information.
- Workforce Training about creation of passwords and passphrases (not easy to guess, use of alpha and numeric when possible).
- Technical controls for workforce members needing access to electronic protected health information including:
    - Which workforce members have access (access profiles).
    - Why access to electronic PHI is permitted.
    - When access to electronic PHI is permitted.
    - When access to electronic PHI is expired.
    - Where access to electronic PHI is permitted.
    - What electronic PHI is permitted access to.
    - How workforce members gain access (includes requiring external/outsourced service providers to identify the functions, ports and protocols used in the provision of services).

2. The Director of Privacy and Data Compliance (DPDC) will ensure that all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications. Once a process and/or technical solution is chosen, the Privacy & Security Officer will assure the solution is implemented in a timely manner and that any affected policies and procedures are updated, and necessary training occurs.
3. The Director of Privacy and Data Compliance (DPDC) will assure that routine monitoring of this solution is carried out in order to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the PHI with its integrity and availability.

Electronic Transmission Security of PHI	
Kansas Health Information Network, Inc. Policies & Procedures	Policy #: 037
Section**:** ***Two*** Subject: ***PSO Policies***	Related Law(s): ***45 CFR § 164.310(d)(1) and 164.312(e)(1)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Next Review Date: January 2025
	Last Reviewed & Updated by: January 2024
Approved by: KHIN Board of Directors	Approval Date: January 17, 2024

Responsibility: Director of Privacy and Data Compliance (DPDC), Systems Support

Policy:

Kansas Health Information Network, Inc. uses a combination of operational policies and technological solutions to ensure the confidentiality, integrity and availability of PHI while it is in transit from one location to another location over an electronic communications network. This type of electronic transmission or movement of PHI includes protection during preparation and during reception and at a minimum use:

- An electronic communications network/local area network with encryption.
- Point to point transmission using a VPN along an open network (such as the internet).
- FIPS-validated cryptographic mechanisms.
- Encrypted Email.

Procedure:

1. The Director of Privacy and Data Compliance (DPDC) will gather all information collected for the risk assessment process relating to all areas of electronic transmission security. This assures that the processes chosen to carry out the security of electronic transmission are in accordance with the level of risk, priority and importance assessed by Kansas Health Information Network, Inc. This compliance material also includes the identification of sensitive data/PHI involved in electronic commerce and on-line transactions as defined as part of the PHI Flow Risk Analysis materials. In this manner, Kansas Health Information Network, Inc. formally documents and authorizes the characteristic of each connection to systems outside of the entity.
2. The Director of Privacy and Data Compliance (DPDC) is responsible to choose the solution by considering the following factors:
    2.1. Reviewing the risk assessment results and related documentation.
    2.2. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.
    2.3. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.
    2.4. Thoroughly considering all areas defined in the procedure as “Implementation Considerations”.

Implementation Considerations Relating to Transmission Security

Consider the business needs for transmission security:

- Kansas Health Information Network, Inc. needs to send electronic PHI over an electronic communications network to providers/brokers/patients/ business associates/employees, and others. This may include transmission of PHI over public networks, private networks and wireless networks.
- Kansas Health Information Network, Inc. need to allow others such as Independent Consultants or customer support functions or others with a business need, remote access.
- Kansas Health Information Network, Inc. enters into appropriate Business Associate Agreements, Third Party Vendor Agreements, Trading Partner and other related types of contractual documents to assure that downstream parties honor privacy/security requirements and service level agreements and comply on an ongoing basis with state/federal laws including but not limited to breach notification.
    - Other agreements with information service and value-added network providers include the same safeguards.
    - Specific transmission protocols and required approval prior to using external public services such as File Sharing and Instant Messaging may be included in these types of documents.
    - Unencrypted PHI should never be sent using "end-user messaging technologies" like Chat; Instant Messaging, and Email and Facsimile (unless the use of more secure channels like secure email or hand delivery are unavailable). SEE Vendor Management and other related policies.
- Consider processes used to gain access:
    - Virtual or dedicated private network.
    - Extranet Virtual Private Network.
    - Wireless Encryption and authentication methods.
    - Instant Messaging; Chat or File Sharing within a controlled network.

Closed Enterprise Network Controls

All communications access to Kansas Health Information Network, Inc. from an open network, such as the Internet and untrusted third-party networks, requires strong authentication.

Communication protocols that will be used when transmitting to and from the Kansas Health Information Network, Inc. include integrity and authenticity of the information (see related technical policies).

Network Perimeter Controls

All access points to untrusted networks shall use some type of security mechanism, which could include, but not be limited to: Firewalls, network address translation device, gateways and proxies.

Open Network Services and the general public

General public access to Kansas Health Information Network, Inc. information is only via connection in a secure manner. Stronger levels of authentication should be in place to enhance access controls from publicly accessible networks. Access only takes place after successful identification and authentication. Cryptography is used to protect PHI handled as part of remote access sessions to the internal network and to external systems.

Encryption Controls

Encryption and decryption use allow for information to be scrambled so that if it were intercepted, it would not be easily understood. It is important for Kansas Health Information Network, Inc. to

determine what level of data is worthy of encryption since overuse can prove financially and technically burdensome. Whenever encryption and decryption are used, the following should be addressed assuring cryptographic mechanisms are in place throughout the duration of the end-to-end transmission:

- Definitive level of algorithm strength.
- Procedure for key generations.
- Key reproduction for emergency access.
- Distribution, storage, use, destruction, and archiving of keys (key management is based on national/international regulations and restrictions and includes specific roles and responsibilities).

Integrity Controls

Integrity is the process of protecting data from improper alteration or destruction during transit.

- Authentication of both users and devices prior to provision of access via wireless systems is required.
- System Activity Review or audit trail logs are recorded for all remote access for all users.
- For Dial-Up:
  - Network systems are checked for unanticipated dial-up capabilities (as applicable).
  - A callback capability with re-authentication is required to verify dial-up connections from authorized locations.
- Use of electronic signatures by each party involved in the transaction is one method to uphold integrity. Legal considerations should be included regarding requirements for use of electronic signature.
- When a trusted authority is used to issue and maintain digital signatures or certificates, security is embedded throughout the end-to-end signature/certificate process.
- The storage of transaction details is not retained and exposed on a storage medium that is directly accessible from the Internet and located outside of any publicly accessible environment.

2. The Director of Privacy and Data Compliance (DPDC) will ensure all decisions related to the solution(s) chosen are well documented and retained in accordance with Kansas Health Information Network, Inc. retention policy. This includes documentation supporting "further assessment" activities in support of "Addressable" Implementation Specifications. Once a process and/or technical solution is chosen, the Director of Privacy and Data Compliance (DPDC) will ensure the solution is implemented in a timely manner and that any affected policies and procedures are updated and training on such occurs as necessary.
   - Technical protocols used for communications are enhanced to handle any new vulnerability (including attacks of the host(s) used for electronic commerce) and the updated versions of protocols are adopted as soon as possible and implemented via standard Change Control processes.
3. The Director of Privacy and Data Compliance (DPDC) will ensure that routine monitoring of this solution is carried out to continually assess the effectiveness of Kansas Health Information Network, Inc. ability to balance the confidentiality of the protected health information with its integrity and availability.