

**Kandiyohi County
Health and Human Services**

**Health Care Insurance Portability and Accountability Act
HIPAA**

Policy

Adopted August 7, 2018

**Kandiyohi County Health and Human Services
HIPAA Policy**

TOPIC	PAGE
Section 1 – Introduction and Purpose	3
Section 2 - Appointment and Duties of Officers	4
Section 3 – Administrative Requirements	4-6
Section 4 – Technical Safeguards	6
Section 5 – Authorized Uses and Disclosures	6-8
Section 6 – Permitted Uses and Disclosures	8-9
Section 7- Welfare Data	9
Section 8 – Requests for Data	10
Section 9- Individual Rights	10-11
Section 10 – Business Associate Relationships	11
Section 11 – Auditing System Activity	11-12
Section 12 – Breach Notification	12-14
Section 13- Risk Assessment and Management	14
Section 14- Social Media	14-15
Definitions	15-17
Signature Page	17

**Kandiyohi County Health and Human Services
HIPAA Policy**

<input checked="" type="checkbox"/> Policy <input type="checkbox"/> Procedure	Division: Health and Human Services	Date Adopted: August 7, 2018
Location: M:\Shared\HIPAA - Information-evaluation\Policy - Procedure\HIPAA PP KCHHS-V3.docx		Date Reviewed: Date Revised:

Original Public Health and Family Service HIPAA Policies were adopted in 2003 and are retired with adoption of this policy.

Section 1 – Introduction and Purpose

The Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 put forth, over years, the [HIPAA Privacy Rule](#), the [HIPAA Security Rule](#) and the [Enforcement Rule](#). The Privacy Rule established national standards for the protection of certain health information. The Security Rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Enforcement Rule established provisions for compliance, investigation and imposition of civil money penalties for violations. HIPAA rules apply to **covered entities** and **business associates**.

HIPAA Privacy Rule: Defines and limits the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either:

- As the Privacy Rule permits or requires, or
- As the individual who is the subject of the information (or the individual’s personal representative(s) authorizes in writing.

HIPAA Security Rule: Requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information (PHI). Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce

HIPAA Enforcement Rule: Requires a HIPAA privacy and security rule complaint process. It also defines the penalty for failure to comply with HIPAA and provisions for enforcing violations. Failure to comply with HIPAA can result in civil and criminal penalties. See HHS.gov:

Reasonable Cause: an act or omission that violates HIPAA not found to be acted with willful neglect.

Reasonable Diligence: prudence expected to satisfy a legal requirement under similar circumstances.

Willful Neglect: conscious, intentional failure or reckless indifference to the obligation to comply with HIPAA.

Civil and criminal penalties for failure to comply

HIPAA Violation	Minimum civil penalty	Maximum civil penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	\$100 per violation, with an annual maximum of \$25,000 for repeat violations	\$50,000 per violation , with an annual maximum of \$1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	\$1,000 per violation, with an annual max of \$100,000 for repeat violations	\$50,000 per violation, with an annual max of \$1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	\$10,000 per violation, with an annual max of \$250,000 for repeat violations	\$50,000 per violation, with an annual max of \$1.5 million
HIPAA violation is due to willful neglect and is not corrected	\$50,000 per violation, with an annual max of \$1.5 million	\$50,000 per violation, with an annual max of \$1.5 million

Kandiyohi County Health and Human Services HIPAA Policy

Who must comply with HIPAA Rules?

- Health Plans
- Health Care clearinghouses: entities that process nonstandard information into a standard format
- Every health care provider, regardless of size, who electronically transmits health information

What types of information does HIPAA protect?

The **HIPAA Privacy Rule** protects most *individually identifiable health information (PHI)* held or transmitted by the organization or its Business Associates in any form or media, whether electronic, paper, or oral. PHI is information, including demographic information that relates to:

- Individual's past, present, or future physical or mental health condition
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual

Who enforces HIPAA?

- OCR- Office of Civil Rights
- DOJ- Department of Justice
- FBI- Federal Bureau of Investigation
- State and local authorities, if requested
- Your clients!

Section 2 - Appointment and Duties of Officers

The organization will designate a privacy officer who is responsible for developing and implementing privacy policies and procedures and a security officer who is responsible for developing and implementing security policies and procedures.

- The Health and Human Services Director is the organization's designated Privacy Officer
- The Network Systems Analyst is the organization's designated Security Officer

Section 3 – Administrative Requirements

Security is Everyone's Responsibility. The following responsibilities are shared by all employees:

- Participating in information security awareness activities/trainings
- Reporting security incidents
- Complying with this policy and all associated privacy and security guidelines and forms
- Protecting Kandiyohi County electronic information assets from unauthorized access, use, distribution, disclosure or destruction

Appropriate Administrative, Technical and Physical Safeguards – All employees will reasonably safeguard PHI from any intentional or unintentional use or disclosure in the following manners:

- Keep all entries to employee workstations secure and locked and follow the organization's Visitor Procedure at all times
- Store records containing PHI securely at all times
- Put working documents that contain PHI away at the end of the day
- Locate printers and fax machines in areas not easily accessible to unauthorized personnel
- Assure that documents containing PHI are not left sitting in the fax machine(s)
- Speak quietly when discussing PHI in any work area and refrain from any discussions in areas where public have access
- Limit PHI shared over the phone to the minimum amount necessary to accomplish the purpose
- Place all documents with PHI in secure shredding/confidential containers prior to disposal
- **USER ACCOUNTS:** Each user will be assigned a unique identifier or User ID. User identification will be authenticated before the electronic system grants access to electronic data.

Kandiyohi County Health and Human Services HIPAA Policy

- **COMPUTER MONITORS:** Computer monitors will be positioned so that unauthorized persons cannot easily view information on the screen. IF that is not possible, monitor screen covers will be used. Employee computer monitor screensavers will be set to “lock” after 5 minutes of inactivity to protect privacy.

Refer to [Kandiyohi County Computer and Network Acceptable Use Policy](#), [Computer Use Agreement](#), and [Kandiyohi County Electronic Device Policy/Agreement](#), for policies and procedures related to electronic device use, computer use and network access and acceptable use. These documents must be reviewed and signed annually by all KCHHS employees.

Minimum Necessary: The organization will make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the purpose for which the request is made. An entire medical record will not be disclosed or requested for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. Minimum necessary requirements do not apply to the following circumstances:

- disclosures to health care providers for treatment purposes
- disclosure to an individual who is the subject of the information
- use or disclosure made pursuant to an authorization
- disclosure to HHS for compliance investigation, review or enforcement
- use or disclosure that is required by law
- use or disclosure required for compliance with HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules

Complaints Policy - The organization will provide a process for individuals to make complaints to the organization concerning its HIPAA privacy regulations policies and procedures, its compliance with those policies or procedures or its compliance with the privacy regulations itself. The Notice of Privacy Practices (NOPP) provided to individuals will include a brief description of how individuals may file a complaint, including the title, phone number and address to contact for further information on the policies for filing a complaint. All complaints will be directed to the Privacy Officer. The Privacy Officer or designee will record complaints in the **HIPAA Complaint Tracking and Resolution Log**. The Privacy Officer will document all complaints received and their disposition.

Anti-Retaliation Policy - The organization will not retaliate against any individual for exercising a right under the HIPAA privacy regulations, or for filing a complaint, participating in an investigation, or opposing any lawful act relation to the privacy regulations.

Documentation and Record Retention- The organization will maintain, until six years after the later of the date of their creation or last effective date, it privacy policies and procedures, its privacy practice notices, disposition of complaints, accounting of disclosures and other actions and activities.

Retention of Audit, Risk Assessment/Management, and BAA Information

- Reports summarizing audit activities shall be retained for a period of six years.
- All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place documentation is maintained for six years.
- All BAA documentation shall be maintained for a period of six years beyond the date of when the BAA relationship is terminated.

Destruction of Protected Health Information- Any medium containing PHI must be properly destroyed. PHI stored in paper, electronic or other format will be destroyed utilizing an acceptable method of destruction after the appropriate retention period has been met.

- Paper documents with PHI: shredding, incineration, pulverization and use of a bonded recycling company.
- Computers: for re-use, reformatting of the hard drive. Disposal- hard drive removal and physically destroyed.
- Back up or data tapes: bulk tape eraser or shredded/pulverized.
- CD or diskette: cut into pieces or pulverized.

Kandiyohi County Health and Human Services HIPAA Policy

All inactive Medical records shredded or purged must be authorized by the Privacy Officer and recorded on the **Authorization for Records Disposal Form** prior to destruction.

Training - The organization will train all members of the workforce on the policies and procedures necessary to comply with the HIPAA privacy and security regulations. Employees will receive initial training at the time of implementation of the policy. Training will be documented using the **HIPAA Training Log**. Additional training will be provided to each new member of the workforce as part of orientation to the organization. All employees will be required to review the organization HIPAA policy on an annual basis, as indicated by a signature on an annual agreement form.

Dissemination of HIPAA Policies and Procedures - The organization will place a copy of its HIPAA Policies and Procedures for public consumption on its web site. All related HIPAA policy forms will be placed electronically in an area accessible by all employees.

Notice: The organization will provide a notice of its privacy practices (NOPP). The notice will contain the following elements:

- Description of the ways in which the organization may use and disclose protected health information and how the individual can get access to the information
- Statement of the organization's duties to protect privacy, provide a notice of privacy practices and abide the terms of the notice
- Description of the individual's rights, including the right to complain to HHS and to the organization if they believe their privacy rights have been violated
- A point of contact for further information and for making complaints to the organization

Notice Distribution: When the organization has a direct treatment relationship with an individual a privacy practice notice will be delivered:

- Not later than the first service encounter by personal delivery (for client visits), by automatic electronic response (for electronic delivery of service) and by prompt mailing (for telephonic service delivery)
- By posting the notice at each delivery site in a clear and prominent place
- In emergency treatment situation, as soon as practicable after the emergency abates
- Notice will be electronically available on organization website

Acknowledgment of Notice receipt: Organization will make a good faith effort to obtain written acknowledgement from clients of receipt of the privacy practice notice. The organization will document the reason for any failure to obtain the client's written acknowledgement. The organization is relieved of the need to request acknowledgement in an emergency treatment situation.

Section 4 – Technical Safeguards

Storage and Transport of Data: The Security Officer will be responsible for maintaining security measures for the protection of PHI assets including:

- Virus and malicious software protection
- Firewalls
- System resource usage
- Transmission security, including a valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) and valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission).
- Clearing, purging and/or destroying electronic media prior to disposal of surplus electronic information assets.
- Implementation and administration of databases, hardware, software, third party tools including cloud-provided services or application and communication infrastructure
- Access controls and user identification authentication
- Coordination and approval of all encryption products

**Kandiyohi County Health and Human Services
HIPAA Policy**

- Maintaining an inventory of all county owned servers, PC's, laptops, tablets, and phones
- Access privilege and removal promptly following departure
- Emergency access/disaster recovery procedure

Section 5 – Authorized Uses and Disclosures

Required Disclosures: Organization must disclose information in only two situations:

1. To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information.
2. To HHS when it is undertaking a compliance investigation or review or enforcement action.

Authorized Uses and Disclosures: Federal HIPAA Law states that an organization is permitted, but not required, to use and disclose protected health information, without an individuals' authorization, for the purposes or situations listed below; however, [Minnesota Health Records Act](#) states:

*A provider, or a person who receives health records from a provider, **may not release** a patient's health records to a person **without**: (1) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release; (2) specific authorization in law; or (3) a representation from a provider that holds a signed and dated consent from the patient authorizing the release. [Minn.Stat 144.294](#)*

Consent must be obtained prior to using or disclosing PHI for the following:

1. For treatment, payment and Health care operations

- **Treatment** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a client and referral of a client by one provider to another.
- **Payment** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
- **Health Care Operations** are any of the following activities:
 - a. Quality assessment and improvement activities, including case management and care coordination
 - b. Competency assurance activities, including health plan performance evaluation, credentialing and accreditation
 - c. Conducting or arranging for medical reviews, audits or legal services
 - d. Specified insurance functions, such as underwriting
 - e. Business planning, development, management and administration
 - f. Business management and general administrative activities of the organization

2. **Decedents:** Federal HIPAA guidelines allow this without authorization; however, Minnesota does NOT. PHI may not be disclosed to a funeral home director without consent. Disclosure to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other function authorized by law is allowed.

3. **Cadaveric organ, eye or tissue donation:** Federal HIPAA guidelines allow this without authorization; however, Minnesota does NOT. PHI may not be disclosed to organ banks for cadaveric organ, eye, bone, tissue and other donation purposes without consent.

4. **WIC:** WIC data is private under Federal WIC Regulations, Section 246.26(d). This regulation restricts the use and disclosure of information from WIC applicants and participants to persons directly connected with the administration or enforcement of the program and the Comptroller General of the United States. At the direction of the Food and Nutrition Service, information obtained under the program may be used for consumer summaries, statistical use, or other types of reporting which does not identify individuals. For the purpose of writing reports, state and federal WIC staff may allow others to have access to summary WIC data.

**Kandiyohi County Health and Human Services
HIPAA Policy**

5. **Marketing:** Marketing is any communication about a product or service that encourages recipients of the communication to purchase or use a product or service. Communication for treatment of the individual
6. **Records relating to Mental Health:** with the following exceptions:
 - For organization’s own training and to defend itself in legal proceedings brought by the individual, to avert a serious and imminent threat to public health or safety, to health oversight organization for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner and as required by law.

Consent Requirements: Refer to [Kandiyohi County Guidelines and Procedures for Minnesota Data Practices Act](#) –for specific guidance related to content requirements for written consent/authorizations. In general, Release of Information **MUST be in plain language and MUST** contain 10 items:

1. Name of Organization
2. Name of Organization Receiving Disclosure
3. Name of Client
4. Reason for Disclosure
5. A description of the information to be used/disclosed that identifies the information in a specific and meaningful fashion
6. Client’s Right to Revoke
7. Statement about the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization
8. Date, Event or Condition of Expiration
9. Signature of Client
10. Date of signature

Section 6– Permitted Uses and Disclosures

Permitted Uses and Disclosures: Instances where disclosure is allowed without authorization:

1. **Opportunity to agree or object:** Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree or object. Refer to [45 CFR 164.512 \(i\)](#)
2. Where the individual is **incapacitated, in an emergency situation, or not available**, the organization may make such disclosures, if in the exercise of their professional judgement, the use and disclosure is determined to be in the best interests of the individual. **There are 6 mandatory documentation pieces for any emergency disclosure: 1-name of person to whom disclosure was made; 2-their affiliation with any healthcare facility; 3-name of the person who disclosed; 4-date of disclosure; 5-time of disclosure; and 6-nature of the emergency**
3. **Incidental use and disclosure:** Certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure is permitted, as long as the organization has applied reasonable safeguards and implemented the minimum necessary standard.
4. **Judicial and administrative proceedings as required by Law** (including statute, regulation, or court orders). Refer to [Minn.Stat 626.556](#) for guidance related to child protection disclosures.
5. **Public Health and Safety- Refer to [45 CFR 164.512\(b\)](#).** The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. Other public health activities include:
 - Reporting adverse events, tracking of products, product recalls and post-exposure to communicable disease
 - Reporting suspected child abuse or neglect
 - PHI disclosure, as needed, to notify an individual at risk of contracting or spreading a disease or condition

Kandiyohi County Health and Human Services HIPAA Policy

- Workplace medical surveillance- disclosure to employer for the purposes of surveillance or evaluation or workplace illness and injury to comply with OSHA, with written notice to the individual that the information will be disclosed.
6. **Health oversight activities-** audits and investigation necessary for oversight of the health care system and government benefit programs such as Medicare and Medicaid
 7. **Law enforcement purposes**
 - As required by law (court ordered, subpoena)
 - Records pertaining to an individual's mental health if the law enforcement agency provides the name of the individual and communicates that the individual is currently involved in an emergency interaction with the law enforcement agency and the disclosure of the record(s) is necessary to protect the health or safety of the individual or of another person.
 - To identify or locate a suspect, fugitive, material witness, or missing person
 - In response to a law enforcement official's request for information about a victim or suspected victim of a crime
 - To alert law enforcement of a person's death, if the organization suspects that criminal activity caused the death
 - When the organization believes that protected health information is evidence of a crime that occurred on its premises
 - In a medical emergency not occurring on its premises, when necessary, to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.
 8. **External Research**, *if the individual does not object*, provided the organization obtains either:
 - Documentation that an alteration or waiver of individual's authorization has been approved by an Institutional Review Board or Privacy Board
 - Representation from the researcher that protected health information is solely to prepare a research protocol and is necessary for the research.
 9. **Communication barriers:** If the organization cannot obtain an individual's consent to use or disclose PHI because of substantial communication barriers and an individual's physician, using his or her professional judgment, infers that an individual consent to the use or disclosure, or the physician determines that a limited disclosure is in the individual's best interests, the organization may permit the use or disclosure.
 10. **Workers' Compensation:** As needed to comply with workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.
 11. **Limited Data Set:** PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited set may be used and disclosed for research, health care operations and public health purposes, provided the recipient enters into a data use agreement promising specific safeguards for the PHI within the limited data set. See [45 CFR 164.514\(e\)](#) for more information. The **Data Use Agreement** is similar to a business agreement, but prohibits re-identifying the information or contacting the individuals. Entities/individuals requesting limited data sets outside of the above specified purposes must complete a **Limited Data Set Request Application** for consideration.

Section 7 – Welfare Data

Welfare system includes the Department of Human Services, local social services agencies, county welfare agencies, and county public health agencies, county veteran services agencies, county housing agencies, private licensing agencies, the public authority responsible for child support enforcement, human services boards, community mental health center boards, state hospital state nursing homes, the ombudsman for mental health and developmental disabilities , Native American tribes to the extent a tribe provides a service component of the welfare system, and person, agencies, institutions, organizations , and other entities under contract to any of the above named agencies to the extent specified in the contract. Data on individuals collected, maintained, used, or disseminated by the welfare system are private data on individuals, and shall not be disclosed without consent. Refer to [Minn.Stat 13.46](#) for guidance related to exceptions for sharing of welfare data without consent or as provided by law.

Kandiyohi County Health and Human Services HIPAA Policy

Data sharing within the organization is allowed when a work assignment reasonably requires access. See [MN Data Practice Act Admin Rules](#). MN statute also allows for sharing of private data between personnel in the welfare system working in the same program. [Minn.Stat 13.46, subd. 2\(a\)\(7\)](#)

Section 8 – Requests for Data

Refer to [Kandiyohi County Guidelines and Procedures for Minnesota Data Practices Act](#) for policies/procedures related to accessing and requesting **government data**, including requests for summary data derived from private or confidential data on individuals and associated forms and fees for copies of government data.

All protected health information (**PHI**) **data requests** shall be documented using the **HIPAA Data Disclosure Request Form**. All PHI Data request forms shall be retained until six years after the date of request. A **designated responsible authority or designee** will be determined to receive and comply with requests for government data for designated departments. When an individual requests a copy of their records for purposes of reviewing current medical care, the organization must not charge a fee. If the request is for records of past medical care, or for certain appeals, the organization may charge a fee.

The organization will comply immediately, if possible, with any request made, or within 10 days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. The organization must maintain an accounting of all disclosures of PHI, other than to the individual, which were made by the organization. Disclosures will be documented using the **HIPAA Data Disclosure Log** or tracked within the electronic health record.

Denying Access: If the organization reasonably determines that the information is detrimental to the physical or mental health of the client, or is likely to cause the patient to inflict self-harm, or to harm another, the organization may withhold the information from the client and may supply the information to an appropriate third party.

Section 9- Individual Rights

Access to data: Individuals have a right to review and/or obtain an electronic or paper copy of their protected health information in the organization's *designated record set*.

Designated record set means a group of records (any item, collection, or grouping of information that includes protected health information) maintained by or for the organization that is:

- a. The medical records and billing records about individual(s)
- b. The enrollment, payment, claims adjudication, and case or medical management records; or
- c. Used, in whole or in part, by or for the organization to make decisions about individuals.

Some information maintained by the organization is not used to make health care decisions, such as audit trails, appointment schedules and practice guidelines that do not imbed PHI, incident reports, quality assurance data, and statistical reports. In accordance with the privacy regulations, the organization is not required to grant an individual access to protected PHI maintained in these types of information systems.

Restricted Use Request: Organization will allow an individual to request that the Organization restricts its use and disclosure of the PHI for treatment, payment or health care operations. The Organization is not required to agree to the restriction; however, if the Organization agrees to the restriction, it will not violate that agreement, except for emergency treatment. Individuals requesting restricted use shall complete **Request Not to Use or Disclose Personal Health Information Form**.

Alternative Means of Communication Request: The Organization will accommodate all reasonable requests from individuals to receive communication of protected the PHI by alternative means or at an alternative location, provided

Kandiyohi County Health and Human Services HIPAA Policy

the individual clearly states that disclosure of all or part of that information could endanger the individual. The request will be documented clearly for any employee working with the client to see.

Request to Amend: An individual subject of the data may contest the accuracy of completeness of the data. Any requests shall be completed in writing by the individual using the ***Request to Correct or Amend Personal Health Information Form***. The organization will either 1) correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or 2) notify the individual that the organization believes the data to be correct. The individual will receive a response using the ***Response to Correct or Amend Personal Health Information Form***.

Accounting of Disclosures: Individuals have a right to receive an accounting of disclosures of their PHI that occurred during the six years prior to the date of the request for an accounting, including disclosures to or by business associates of the organization. To request, the individual must complete the ***Request for Accounting of Disclosures Form***.

Accounting of disclosures must list:

- Names of persons or entities to whom PHI was disclosed
- Date on which the PHI was disclosed
- Description of the PHI disclosed
- Purpose of the disclosure

Section 10 – Business Associate Relationships

The organization may disclose PHI to another entity if it receives satisfactory assurances, provided in a written contract (***Standard BAA Agreement***), that the business associate will appropriately safeguard the PHI. If the Organization and business associate are both governmental entities, a memorandum of agreement will provide satisfactory assurances. The Director or designee is responsible for maintaining an accurate list of BAA agreements held by the organization.

Obtaining Satisfactory Assurances in Contracts - The contract or other written arrangement will provide satisfactory assurances to the Organization that the business associate will comply with HIPAA requirements necessary to protect the protected PHI shared by the organization. The contract or other written arrangement will establish permitted and required uses and disclosures.

Documenting Sanctions for Non-Compliance - The contract or other written arrangement will authorize termination if the business associate violates its terms. If the Organization knows of a pattern of non-compliance with HIPAA by the business associates, the Organization realizes it will be found to be non-compliant unless the Organization took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

- Terminated the contract or arrangement, if feasible; or
- If termination is not feasible, reported the problem to the Department of Human Services.

The organization may serve as a BA to another covered entity and may be asked to review and sign that covered entity's external BA agreement/addendum or contract. As a BA, the organization should:

- Forward the external information to the Privacy Officer to review the submitted BA agreement to ensure that the provisions outlined are consistent with those set forth in this policy.
- If the BA agreement is not consistent with this policy or contains additional provisions or provisions that are inconsistent with the privacy regulation, the Privacy Officer may recommend the following alternatives.
 - Agree to the additional provisions and sign the agreement.
 - Refer the agreement to legal counsel to determine appropriateness before signing.
 - Refuse to agree to the provisions and notify the covered entity to establish a resolution.

Section 11 – Auditing System Activity

Audit Controls: Organization will implement hardware, software, and/or procedural mechanisms that record and examine access and other activity in information systems that contain or use PHI. The organization will consider risk,

Kandiyohi County Health and Human Services HIPAA Policy

vulnerability and organizational factors to determine reasonable and appropriate audit controls. Information systems that contain or use PHI will have ability to detect, report, and guard against:

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

At a minimum, organization will provide immediate auditing in response to:

- Client complaint
- Employee complaint
- Suspected breach of patient confidentiality
- High risk or problem prone event (e.g., VIP admission)
- Any action that causes suspicion or poses a concern

Evaluation and Reporting of Audit Findings: Significant findings will be reported immediately in a written format to the Privacy Officer. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken.

Audit Logs: Audit logs will be protected from unauthorized access or modification, so the information they contain will be available if needed to evaluate a security incident. Whenever possible, audit trail information will be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails. Audit logs maintained within an application will be backed-up as part of the application's regular backup procedure.

Back-up and Recovery: Information Technology Department will maintain data backup guidelines to define the process for the secure backup and storage of data files and software both onsite and offsite. Auditing of data back-up processes will be carried out:

- On a periodic basis (at least annually) for established practices and procedures.
- More often for newly developed practices and procedures

Integrity: Integrity of organization's PHI will be protected from improper alteration or destruction. Electronic mechanisms that house PHI must have available functions or processes that automatically check for data integrity to minimize unintentional alteration or destruction of PHI.

Section 12 – Breach Notification

Breach is defined as an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. Refer to [***Kandiyohi County Guidelines and Procedures for Minnesota Government Data Practices Act***](#) for Organization Breach Protocols related to private or confidential data breaches. See

Breach of unsecured PHI- A miss-use or disclosure of PHI is presumed to be a breach unless the organization or BA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

There are **3 exceptions** to the definition of a breach:

1. The unintentional acquisition, access, or use of PHI by a workforce member, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. The inadvertent disclosure of PHI by a person authorized to access PHI in the organization or BA to another person authorized to access PHI in the organization or BA or organized health care arrangement in which the

Kandiyohi County Health and Human Services HIPAA Policy

organization participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

3. The organization or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Potential Breach Discovery/Reporting- Any employee who knows of or reasonably believes a breach of PHI may have occurred must immediately report to his or her supervisor and/or to the designated Privacy Officer in writing by completing the **Potential Protected Health Information Data Breach Report**. The notification should include:

- Date and time of report
- When the breach occurred (if known)
- Type of PHI involved
- Approximate number of affected individuals

Breach Determination- Following the discovery of a potential breach, the Privacy Officer and/or Security Officer will conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. The organization will also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.). The organization may make breach notification without completing a risk assessment.

Documentation- Privacy Officer or Security Officer will document how determination was made of a breach and decisions around notifications using the **Breach of Security Incident Response Summary** form. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. The organization will maintain a log of all breaches which will include:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known.
- A description of the types of unsecured PHI involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
- A description of the action taken with regard to individual notification, the media, and the Secretary regarding the breach
- Description of the breach determination was made
- Steps taken to mitigate the breach and prevent future occurrences

Breach Notification Requirements- Individual notification must be provided without reasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible:

- A brief description of the breach
- A description of the types of information involved in the breach
- The steps the individuals should take to protect themselves from potential harm
- A brief description of what the organization is doing to investigate the breach, mitigate the harm and prevent future breaches
- Contact information for the organization

Notice must be in written form by first class mail or e-mail (if the affected individual has agreed to receive such notice electronically).

- If the organization has insufficient or out-of-date contact information for 10 or more individuals, the organization must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing notice in a major print or broadcast media where the affected individuals likely reside. The organization must include a toll-free number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
- If the insufficient or out-of-date contact information is for fewer than 10 individuals, the organization can provide substitute notice by an alternative form of written notice, by telephone, or other means.

Kandiyohi County Health and Human Services HIPAA Policy

- **Sample notification letters** are included with HIPAA Policy forms.

Media Notice- A breach affecting more than 500 residents of a state or jurisdiction requires notification to the individual AND to prominent media outlets serving the state or jurisdiction, likely in the form of a press release. This notification follows the same information requirements and time parameters as noted above.

Notice to the Secretary of HHS- In addition to notifying affected individuals and the media (where appropriate), the organization will notify the Secretary by visiting the HHS web site and filling out and [electronically submitting a breach report form](#). If a breach affects 500 or more individuals, the organization will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the organization will notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

Business Associate Responsibilities- If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the organization following the discovery of the breach. A business associate must provide notice to the organization without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the organization with the identification of each individual affected by the breach as well as any other available information required to be provided by the organization in its notification to affected individuals.

Section 13 – Risk Assessment and Risk Management

The organization will follow two standard information security processes- **Risk Assessment** and **Risk Management**.

Risk Assessment: The organization will conduct annually and as needed Risk Assessments to prevent, detect, contain, and correct security violations. The risk assessment provides an accurate and thorough assessment of the potential risks, threats and vulnerabilities to the confidentiality, integrity and availability of PHI held by the organization.

Risk includes the likelihood of a given threat triggering a vulnerability and the resulting impact on the organization. The risk assessment will identify “trigger events” that raise awareness of questionable conditions of viewing confidential information.

Threats are commonly categorized as:

- Environmental – power failures, pollution, chemicals, and liquid leakage
- Human – caused or enabled by humans and may include intentional (network and computer based attacks, malicious software upload and unauthorized access to PHI) or unintentional (inadvertent data entry or deletion and inaccurate data entry) actions.
- Natural – fires, floods, electrical storms, tornados, etc.
- Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
- Other – explosions, medical emergencies, misuse or resources, etc.

Vulnerabilities are categorized as:

- Technical-holes, flaws or weaknesses in the development of information systems or incorrectly configured information systems
- Non-technical- ineffective or non-existent policies, procedures, standards or guidelines

There is no single method or “best practice” for performing a risk assessment that guarantees compliance with the Security Rule. The organization will document the assessment process using the **Risk Assessment Form** and will involve identified staff from different work areas. Upon completion of the assessment, a risk management plan will be developed and documented on the **Risk Management Form**. See [Security Risk Assessment Tool](#) for an optional tool for risk assessment.

Kandiyohi County Health and Human Services HIPAA Policy

The risk assessment process will include the following activities:

- Evaluation of the likelihood and impact of potential risk to PHI
- Implementation of appropriate security measures to address the risk identified
- Documentation of the chosen security measures and the rationale for adopting those measures
- Maintenance of continuous, reasonable and appropriate security protections

Risk Management: Organization will implement security measures sufficient to reduce identified risks and vulnerability to a reasonable and appropriate level by following the following steps:

1. Development and implementation of a risk management plan
2. Implementation of security measures
3. Evaluation and maintenance of security measures

Section 14 – Social Media

The following are guidelines for KCHHS's employees who participate in social media. Social media includes personal blogs and other websites, including Facebook, LinkedIn, Twitter, YouTube or others. These guidelines apply whether employees are posting to their own sites or commenting on other sites:

- Follow all applicable Data Privacy and HIPAA policies. For example, you must not share confidential or private information about KCHHS and you must maintain consumers and patient privacy.
- Write in the first person. Where your connection to KCHHS is apparent, make it clear that you are speaking for yourself and not on behalf of KCHHS.
- Ensure that your social media activity does not interfere with your work commitments.
- KCHHS strongly discourages “friending” of consumers/patients on social media websites. Staff generally should not initiate or accept friend requests except in unusual circumstances such as the situation where an in-person friendship pre-dates the professional relationship.

Definitions

Access: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.

Administration: Defined as administrative staff of KCHHS, which includes the Director and supervisory staff.

Audit: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing. Audit activities shall also take into consideration KCHHS information system risk assessment results.

Audit Controls: Technical mechanisms that track and record computer/system activities.

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

Audit Trail: Means to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events (audit logs) that relate to an operating system, an application, or user activities. *An audit trail identifies **who** (login) did **what** (create, read, modify, delete, add, etc.) to **what** (data) and **when** (date, time).*

Business Associate (BA): A person (or entity) who is not a member of the organization’s workforce and who performs any function or activity involving the use, disclosure, creation or reception of individually identifiable health information

Kandiyohi County Health and Human Services HIPAA Policy

(PHI) or who provides services to a covered entity that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc.

Business Associate Agreement (BAA): A legally binding agreement entered into by a covered entity and business associate that establishes permitted and required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. Refer to [45 CFR § 164.502\(e\)\(1\)](#) to determine when the standard is not applicable.

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

Designated Record Set: A group of records maintained by the organization that is: a) the medical records and billing records about individuals; b) the enrollment, payment, claims adjudication, and case management record systems; c) used, in whole or in part, by or for the organization to make decisions about individuals.

Designee: Any person designated by the Privacy Officer or Privacy Official to be in charge of individual files or systems containing data and to receive and comply with requests for and accounting of data or any other duties related to this Policy.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

HIPAA: HEALTH CARE INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Law Enforcement Official: Any officer or employee of an organization or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Organization: For the purposes of this policy, the term “organization” shall mean KCHHS to which this policy applies.

Personal Representative - someone who has, under applicable law, the authority to act on behalf of an individual in making decisions related to health care.

Privacy Officer: Personnel designated to develop and implement privacy policies and procedures.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. **Individually Identifiable Health Information** is a subset of health information, including demographic information collected from an individual, 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 identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Record: any item, collection, or grouping of information that includes protected PHI data and is maintained, collected, used or disseminated by the organization.

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

Risk Assessment: (Referred to as *Risk Analysis* in the HIPAA Security Rule). Process to prevent, detect, contain, and correct security violations that results in recommended possible actions/controls that could reduce or offset the determined risk.

**Kandiyohi County Health and Human Services
HIPAA Policy**

Risk Management: Sometimes referred to as *Risk Mitigation*, is identified as a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within the organization given its mission and available resources.

Security Officer: Personnel designated to develop and implement security policies and procedures.

Threat: the potential for a particular source to successfully exercise a particular vulnerability.

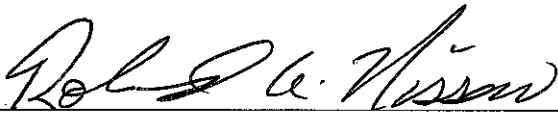
Threat Source: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system.

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

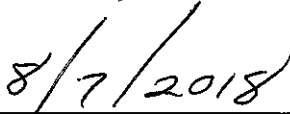
Unsecured Protected Health Information: Protected health information (PHI) that is rendered unusable, is unreadable, or indecipherable to unauthorized persons through the use of technology or methodology.

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

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



Roland Nissen, Chair
Kandiyohi County Board of Commissioners



Date

Date Adopted: August 7, 2018

Date Effective: August 7, 2018