Clay County Social Services

HIPAA Privacy and Security Policies and Procedures

Policy Owner: Clay County Social Services Department Head

Effective Date: March 19, 2024
Approved by the Clay County Board of Commissioners

Table of Contents

Title **Page**

INTRODUCTION

The privacy and security rules under the Health Insurance Portability and Accountability Act and its implementing regulations (collectively, "HIPAA") apply to individuals and organizations designated under HIPAA as "covered entities". Covered entities include: (i) *health care providers* who conduct certain transactions electronically, including but not limited to transmission of health care claims, health care payments, enrollment in a health plan, and referral authorizations; (ii) *group health plans*; and (iii) *health care clearinghouses*.

Clay County Social Services ("Covered Entity" or "Clay County") performs activities that bring it within the definition of a covered health care provider under HIPAA. In addition, certain state privacy laws may apply to Clay County's services.

It is Clay County's policy to maintain the privacy of Protected Health Information ("PHI") received in the course of providing services. To that end, Clay County will comply with the HIPAA privacy standards as outlined in this manual of HIPAA Policies and Procedures ("Policy") and in the Business Associate Agreements between Clay County and various business partners.

This Policy supersedes and replaces any prior HIPAA policies and procedures of Clay County, and is in effect as of the Effective Date.

The following policies shall be referenced and incorporated into this Policy:

- Clay County Social Services Federal Tax Information (FTI) and Social Security Administration (SSA) Safeguarding Requirements, effective May 19, 2022 ("FTI and SSA Safeguarding Requirements Policy");

- Clay County Social Services Compliance Reporting Policy, last updated September 20, 2021 ("Compliance Policy");

- Clay County Social Services New Employee Orientation Policy & Procedure Manual, last updated September 28, 2021 ("New Employee Orientation Policy");

- Clay County Incident Management and Response Plan, last updated September 6, 2023 ("Clay County Incident Response Plan");

- Disaster Recovery Plan For The Clay County Electronic Data Systems, effective as of March 2022 (“Disaster Recovery Plan”);

- Clay County Personnel Policy, last updated January 1, 2024;

- Clay County Acceptable Use Policy, last updated January 21, 2020;

- County Human Services General Records Retention Schedule, last updated April 26, 2022;

- Health Care Bill of Rights for Mental Health Services Policy, last updated March 1, 2021 (“Bill of Rights Policy”); and

- Clay County 2024 Data Practices Policies for Data Subjects and the Public, found here https://claycountymn.gov/1437/Data-Practices (“Data Practices Policies”) (collectively, “Referenced Policies”).

To the extent that there is a conflict between the obligations described in Referenced Policies, and/or this Policy, the more restrictive obligations shall prevail.

DESIGNATION OF PRIVACY AND SECURITY OFFICERS

Designation of Privacy and Security Officers:

Clay County designates the following individuals as its Privacy Officer and Security Officer:

Designated Privacy Officer for Clay County Social Services Department

- Clay County Social Services Department Head

Designated Security Officer for Clay County Social Services Department

- Technology Services Director

Designated Privacy Officer for Clay County as a whole (“Clay County General Privacy Officer”)

- Clay County Administrator

DEFINITIONS

Unless the context otherwise requires, the following terms shall have the meaning set forth below when used in these Policies and Procedures, regardless of whether the term is capitalized or lower case.

Authorization	Written permission
Breach	A breach is the impermissible use, access, acquisition, or disclosure of Unsecured PHI under the HIPAA which compromises the security or privacy of PHI. Three exceptions to the definition of Breach exist. The first exception provides that the unintentional acquisition, access, or use of PHI by a Workforce Member acting under the authority of a covered entity or business associate is not a Breach. The second exception provides that the inadvertent disclosure of PHI at a covered Entity or Business Associate to another person authorized to access the PHI at the same entity is not a Breach. Finally, the third exception allows that no Breach has occurred where the unauthorized individual is not capable of retaining the impermissibly disclosed PHI.
Business Associate	A Business Associate is a person or entity, other than a Workforce Member of the Covered Entity, who performs functions or activities on behalf of the Covered Entity that involve access by the Business Associate to PHI, including the creation, reception, transmission, or maintenance of PHI. Persons or organizations providing these services are Business Associates only if they need more than just an incidental access to PHI in order to perform the services or if they maintain PHI on behalf of a Covered Entity and have the persistent opportunity to access such PHI. **Examples of services where a person or organization may need access to PHI:** o Legal services o Actuarial services o Accounting services o Consulting services o Data aggregation services (Utilization review, quality assurance) o Management services o Administrative services

	○ Accreditation services ○ Financial services (claims processing or administration, billing)
Covered Entity	Is defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
De-identification	The process by which PHI is rendered individually unidentifiable through removal of the 18 identifiers identified under HIPAA or through a determination based upon statistical and scientific methods.
Designated Record Set	As defined under the Privacy Rule at 45 C.F.R. § 164.501, means a group of records maintained by or for a Covered Entity, such as: (a) the medical records and billing records about individuals maintained by or for a covered health care provider; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health care plan; or (c) used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
Device	Any electronic computing device Processing ePHI (whether held onsite or offsite) that is owned, provided by, or otherwise used to access Clay County Systems, which may include desktop computers, laptops, portable electronic devices such as smartphones and tablets, and any peripheral equipment including monitors, printers, digital cameras, and projectors.
Disclosure	The release, transfer, provision of access to, or divulging in any other manner of information to another organization, agency, or person.
Electronic Health Record	Has the same meaning that applies under Section 13400(5) of HITECH and currently means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized staff.
Electronic Media	Means: (a) Electronic storage media including memory devices in computers (hard drives) and any removable / transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

	(b) Transmission media used to exchange information already in electronic storage media, which may include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media; or (c) Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.
Electronic Protected Health Information (e-PHI)	As defined by 45 C.F. R. §160.103, means individually identifiable health information that is transmitted by electronic media, or maintained in electronic media, but not certain education and employment records as described in 45 C.F.R. § 160.103, the definition of Protected Health Information. EPHI also includes any e-PHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity.
Encryption	Encryption is the use of an algorithmic 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.
Health Care Operations	Activities that support the core functions of a Covered Entity, including administrative, legal, financial, and quality improvement activities. This definition shall be interpreted consistent with the definition contained within the HIPAA privacy rules.
HHS	The U.S. Department of Health and Human Services.
HIPAA	Health Insurance Portability and Accountability Act, including applicable regulations at 45 CFR Parts 160 and 164.
HITECH	Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act (ARRA Public Law 111-5 Title XIII of ARRA was given a subtitle: Health Information Technology for Economic and Clinical Health Act (HITECH)).

Individual	The person who is the subject of Protected Health Information. It also includes a person who qualifies as a Personal Representative in accordance with 45 C.F.R. §1264.502(g).
Information	Data pertaining to the individuals, to their circumstances and to the services provided to them. Information regarding individuals created or maintained by the Covered Entity belongs to the Covered Entity and all representatives of the Covered Entity are responsible for holding it in confidence. Confidentiality pertains to information in all of its possible forms (written, oral, and electronic).
OCR	Health and Human Service's Office of Civil Rights
Payment	Uses or disclosures made for payment include those made to obtain payment or seek reimbursement for services rendered.
Privacy Rule	Means the Standards for Privacy of individually Identifiable Health Information codified at 45 C.F.R. §§ 160 and 164, Subpart E, any other applicable provision of HIPAA, and any amendments to HIPAA, including HITECH.
Privacy Officer	Means the person who oversees the development, implementation, maintenance of, and adherence to privacy policies and procedures.
Process	Means the act of accessing, collecting, creating, receiving, using, maintaining, disclosing, or transmitting ePHI.
Program Leader	Workforce Member responsible for the oversight of an applicable Clay County program or department. To the extent applicable, the Privacy Officer, may serve as the "Program Leader" for purposes of this Policy.
Protected Health Information (PHI)	Individually identifiable health information that is transmitted or maintained in written, electronic, verbal/sign language, or any other media that reveals the state of a person's health; that identifies a person in such a way that it gives reasonable basis for determining a person's identity; and that is created or received by a health care provider. PHI includes, without limitation, any PHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use of PHI shall apply equally to ePHI.

Record	Any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.
Re-identification	The process of assigning a code or other means of record identification in order to allow de-identified PHI to be identified but still maintaining the anonymity of the individual described in the procedure contained in this Policy.
Restriction	An agreed upon limitation on the use and disclosure of PHI about an individual in order to carry out treatment, receive payment, or health care operations; or to individuals assisting in the person's care; or to friends, caregivers, or family members for notification purposes.
Security Incident	As defined by 45 C.F.R. § 164.304 means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Security Officer	Is responsible for the continuous management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all organizational information systems.
Security Rule	Means the Security Standards for the Protection of Electronic Protected Health Information codified at 45 C.F.R. §§ 160 and 164, Subpart C, any other applicable provision of HIPAA, and any amendments to HIPAA, including HITECH.
System	Any system, network, platform, database, computer, operating environment, or telecommunications or other information system owned, controlled, or operated by or on behalf of the Clay County and shall include any Device, telework, or remote systems, and/or any Electronic Media.
Treatment	The provision, coordination, or management of health care and related services.
Unsecure PHI	Unsecured PHI is PHI subject to the HIPAA Privacy Rule, which is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or a methodology specified by the HHS in guidance, such as National Institute of Standards and Technology (NIST) standards for destruction.
Use	Information used internally within the organization and not externally disclosed.

Workforce Members	Employees, volunteers, trainees, and other persons under the direct control of the Covered Entity, whether or not paid on Covered Entity's payroll.

PRIVACY OFFICER DUTIES

The duties of the Privacy Officer are as follows:

1. Coordinate privacy activities of Clay County, including development, implementation, maintenance of policies and procedures on privacy, confidentiality, and disclosure of PHI, including the Policy.

2. Review new or revised laws and regulations pertaining to the HIPAA Privacy Rule to determine if new policies or modifications to the Policy is needed.

3. Conduct internal privacy audits and compliance audits on a periodic basis.

4. Ensure that HIPAA privacy training is provided to all Workforce Members who have access to PHI.

5. Ensure Clay County has and maintains appropriate authorization forms, privacy notices, and other related materials reflecting current organization and legal requirements.

6. Review compliance with the HIPAA Privacy Rule and coordinate with Program Leaders to enforce sanctions for failure to comply with privacy policies, including this Policy.

7. Review and answer questions or issues raised by Clay County Workforce Members regarding the proper privacy practices in a particular situation.

8. Cooperate with law enforcement or government agency personnel in any compliance reviews or investigations regarding the HIPAA Privacy Rule.

9. Manage all inquiries and requests regarding privacy.

The responsibilities of the Privacy Officer shall cease immediately upon such individual's resignation as the Privacy Officer or upon termination of employment from Clay County. Clay County will take all reasonable steps to replace the named Privacy Officer as soon as practicable upon such resignation or termination of employment.

PROTECTED HEALTH INFORMATION (PHI)

Protected Health Information (PHI) is individually identifiable health information created or received by Clay County that relates to the past, present, or future physical or mental health condition of the individual, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual. Clay County may create, receive, use, or disclose PHI to carry out its services and to receive reimbursement for the provisions of such services.

The chart below shows: (i) the different healthcare programs offered by Clay County, (ii) the categories of PHI created, maintained, received, used, and/or disclosed by Clay County within each program, (iii) where PHI is stored, and (iv) in what circumstances PHI is received and shared ("management of PHI"). All other PHI is created, maintained, received, used, and/or disclosed by a business associate. PHI is only provided to Workforce Members with a "need to know", (e.g., employees who require knowledge of relevant PHI in order to conduct their jobs and provide the services with which they are tasked).

Table - Description of Clay County Processing Activities

Program	On-Going Child Protection Division	Child Intake and Assessment Division	Children's Mental Health and Child Welfare Division	Behavioral Health and Adult Protection Division	Home & Community Based Services Division	Licensing and Disability Division	Financial Services Division	Child Support, Fraud and Collections Division	Office Support Division
Program Description	**Programs:** *Child Protection & Child Welfare Case Management *Permanency and Adoption *Out of Home Placements *Child in Need of Protection Court Petitions *Minor Parent Case Management *Supervised Visitations	**Programs:** *Intake *Child Protection Investigations *Family Assessment Investigations *Parent Support Outreach *Emergency Placements *CHIPS Petitions	**Programs:** *Child Protection & Child Welfare Case Management *Children's Mental Health *Voluntary Out of Home Placements *Children's Mental Health Respite Referrals *Volunteer Driver Program *Home and Community Based Waiver Services for Children's Mental Health.	**Programs:** *Adult Mental Health Case Management *Pre-Petition Screening & Commitments *Substance Use Comprehensive Assessments & Treatment Coordination *Adult Protection Investigations	**Programs:** *Developmental Disabilities Case Management *Medicaid Waiver Case Management -CAC, CADI,TBI, DD *Semi Independent Living Skills referral and funding *Day Training & Habilitation referral and funding *Consumer Support Grant *Family Support Grant	**Licensing** **Programs** *Day Care Licensing & recruitment *Child Foster Care Licensing & recruitment *Adult Foster Care Licensing & recruitment *Long Term Services & Supports MnChoices Assessments *Special Needs Basic Care Coordination *Adult/Disability Intake & Referrals	**Programs** Administer the following state and federal programs: *MFIP *Employment & Training (Rural MN CEP) *DWP *GA *MSA *GRH *RCA *SNAP *Child Care Programs *Medical Assistance *MA Access Transportation *Emergency Cash Assistance *County Funded Burials	**Programs:** *Locate Parents *Establish parentage *Establish court orders *Enforce, review & modify orders *Collect payments *Fraud and criminal investigations *Collect county debt *Enforce probate cases *Act as Rep. Payee *Facilitate paternity testing	Support the work of all the units, handle front reception areas, phones, mail, etc.

	On-Going Child Protection Division	Child Intake and Assessment Division	Children's Mental Health and Child Welfare Division	Behavioral Health and Adult Protection Division	Home & Community Based Services Division	Licensing and Disability Division	Financial Services Division	Child Support, Fraud and Collections Division	Office Support Division
PHI Categories	● Name ● Date of birth ● Physical and mental Health (including psychiatric evaluations), Drug and Alcohol, and other Medical records are received from providers, other programs, clients, and client family members ● Social Security Number and other government IDs ● Criminal and legal history ● School / education history ● Work history ● Household information ● Financial information, including wages and expenses ● Race/ethnicity & military status ● Illness / Disability information ● Immigration information ● Contact information ● Marital status								
Storage of PHI	● *Paper records*: are stored in locked cabinets in secure office areas with access restricted to only those who have a need to have the paper documents. ● *Electronic records*: are stored in an electronic document management system called CaseWorks which is held on Clay County systems.								
Management of PHI	● *Records received from and shared with*: Various internal departments as well as outside entities such as client family members and representatives, medical and/or mental health service providers, schools, court officials, law enforcement, related government, non-profit and private agencies, health care insurers, credit bureaus / creditors, medical examiners / coroners, and auditors/investigators ● *Purpose of sharing*: to provide services, refer clients to other entities for services, and legal purposes								

DE-IDENTIFICATION OF PHI

1. PURPOSE – To establish policy and procedures for determining when health Information is not individually identifiable or for the de-identification of PHI, and for the subsequent re-identification.

2. Clay County may determine when health information is not individually identifiable or when to de-identify PHI for disclosures other than for healthcare purposes in accordance with the HIPAA. Clay County may also determine when it is necessary to re-identify previously de-identified PHI. Clay County must comply with the terms of this Policy to adequately de-identify PHI and to ensure proper re-identification of PHI.

3. PROCEDURE – Clay County shall determine whether health information should remain individually identifiable or be de-identified. This determination will be made on a case-by-case basis depending on the nature of the request and whether there is a "need to know" the identity of the individual. There are two methods Clay County may use to ensure that health information has been de-identified. The first method includes retaining an expert experienced with generally accepted statistical and scientific principles and methods for rendering de-identified information who determines and documents that the de-identification method employed by Clay County shows little risk that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient of the information to identify the subject information.

   The second method requires removing 18 different identifiers from the information. All of the following must be removed to de-identify health information:

   - Names (individual, relatives, household members)
   - Dates (birth date, date of admission, discharge, etc.)
   - Social Security Number
   - Address, including ZIP code
   - Employer
   - Telephone and fax numbers
   - Email addresses
   - Account number
   - Medical record number
   - Health plan ID numbers
   - Health care beneficiary numbers
   - Certificate numbers
   - Device numbers
   - Vehicle identifiers and serial numbers
   - License number
   - Photographs
   - Fingerprints or voice prints
   - Web Universal Resource Locators (URL's)
   - Internet Protocol (IP) address numbers
   - Biometric identifiers

- Full face photographic images and any comparable images
- Other unique identifiers

Clay County cannot have actual knowledge that any information used alone, or in combination with any other information, would identify an individual who is a subject of the information.

4. Medical records code assignments can be used to “re-identify” the de-identified data as long as the code is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual. Clay County must not use or disclose the code or any other means of record identification for any other purpose and must not disclose the mechanism for re-identification.

PERMITTED USES AND DISCLOSURES OF PHI

Under HIPAA, PHI may be used and disclosed without individual authorization under HIPAA for (i) treatment, (ii) payment for treatment, or (iii) "health care operations" purposes.

"Health care operations" include any of the following activities: (i) quality assessment and improvement activities, including case management and care coordination; (ii) competency assurance activities, including provider performance evaluation, credentialing, and accreditation; (iii) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (iv) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (v) business planning, development, management, and administration; and (vi) business management and general administrative activities, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Unless an exception under HIPAA applies, all other uses and disclosures shall require a HIPAA-compliant authorization. See the "Authorization to Use or Disclose PHI" section below for further information on HIPAA-compliant authorizations.

Please note that state medical confidentiality laws may impose more stringent requirements than those posed under HIPAA. Please see Appendix I **–** State Privacy and/or Confidentiality Laws for further information on permitted uses and disclosures under Minnesota law. To the extent that state law is more stringent than HIPAA, the state law requirement should be followed.

PERSONS THAT NEED ACCESS TO PHI TO CARRY OUT THEIR JOB DUTIES

Workforce Members within Clay County with a "need to know", as determined by the applicable Program Leader, shall be the only ones given access to PHI without additional specific, written authorization by the individual. Program Leaders are responsible for identifying the Workforce Members within their programs or department who need access to PHI to carry out their duties, and for designating the types of PHI needed by each Workforce Member or group to carry out their work duties.

All Clay County Workforce Members shall be informed of the vital importance of confidentiality during their orientation and shall sign a statement indicating their understanding and agreement to abide by the requirements regarding confidentiality.

Workforce Members must review and sign the "Confidentiality Agreement" (see Appendix II, Form 1).

SPECIAL SITUATIONS

HIPAA describes certain "special situations" where a covered entity (i) can use and disclose PHI without individual Authorization in limited situations or (ii) must impose

additional protections with respect to the use and disclosure of PHI. If a "special situation" may apply, the applicable Program Leader or their designee will notify the Privacy Officer of the particular situation, and the Privacy Officer will review whether the use or disclosure is permissible under HIPAA and state medical confidentiality laws prior to any such use or disclosure being made. The Privacy Officer will review this Policy and any applicable documents, and may consult with legal counsel to determine whether HIPAA, and/or state law permits the use or disclosure in the circumstances that are presented. Further information on different special situations enumerated under HIPAA are further described below.

Please note that state medical confidentiality laws may not include the same exceptions provided under HIPAA. Please see Appendix I – State Privacy and/or Confidentiality Laws for further information on permitted exceptions to the authorization requirement under Minnesota law.

Limited Exceptions to the Authorization Requirement

HIPAA provides limited circumstances where individual Authorization is not required to use or disclose PHI, which are further described below.

1. Disaster Relief. Clay County may disclose PHI about an individual to an organization assisting in a disaster relief effort.

2. As Required By Law. Clay County may disclose PHI when required by law to do so.

3. Public Health Activities. Clay County may disclose PHI for public health activities. These activities may include, for example:

   (a) reporting to a public health or other government authority for preventing or controlling disease, injury, or disability; reporting child abuse or neglect; or reporting births and deaths;
   (b) reporting to the federal Food and Drug Administration (FDA) concerning issues such as problems with products or for recall of a product; or
   (c) notifying a person who may have been exposed to or at risk of spreading a communicable disease, if authorized by law.

4. Reporting Victims of Abuse, Neglect, or Domestic Violence. If Clay County believes that an individual has been a victim of abuse, neglect or domestic violence, Clay County may use and disclose PHI to notify a government authority, if authorized by law or if the individual agrees to the report.

5. Health Oversight Activities. Clay County may disclose PHI to a health oversight agency for activities authorized by law. These may include, for example, audits, investigations, inspections, and licensure actions. These activities may include government oversight of the health care system, government payment or regulatory programs, and compliance with civil rights laws.

6. Judicial and Administrative Proceedings. Clay County may disclose PHI in response to a court or administrative order. Clay County also may disclose PHI in response to a subpoena, discovery request, or other lawful process; efforts must be made to contact the individual about the request or to obtain an order or agreement protecting the information.

7. Law Enforcement. Clay County may disclose PHI for certain law enforcement purposes, including, for example, to comply with reporting requirements or report emergencies or suspicious deaths; to comply with a court order, warrant, or similar law enforcement legal process; to identify or locate a suspect or missing person; or to answer certain requests for information concerning crimes or suspected terrorist activity.

8. Research. PHI may be used for research purposes, but only if the privacy aspects of the research have been reviewed and approved by a special Privacy Board or Institutional Review Board, or if the researcher is collecting information in preparing a research proposal, or the research occurs after the death of the individual and the researcher makes certain assurances, or if the individual authorizes the use or disclosure. Note that information is no longer considered PHI once an individual has been deceased for 50 years.

9. Coroners, Medical Examiners, Funeral Directors, Organ Procurement Organizations. Clay County may release PHI to a coroner, medical examiner, funeral director or, in certain instances, to an organization involved in the donation of organs and tissues.

10. To Avert a Serious Threat to Health or Safety. When necessary to prevent a serious threat to an individual's health or safety or the health or safety of the public or another person, Clay County may use PHI or disclose PHI to individuals that are able to help lessen or prevent the threatened harm, such as law enforcement.

11. Military and Veterans. With respect to a member of the armed forces, Clay County may use and disclose PHI as required by military command authorities. Clay County may also use and disclose PHI about foreign military personnel as required by the appropriate foreign military authority.

12. Workers' Compensation. Clay County may use or disclose PHI to comply with laws relating to workers' compensation or similar programs.

13. National Security and Intelligence Activities; Protective Services for the President and Others. Clay County may disclose PHI to authorized federal officials conducting national security and Intelligence activities or as needed to provide protection to the President of the United States, certain other persons, or foreign heads of states or to conduct certain special investigations.

14. Inmates/Law Enforcement Custody. If an individual is an inmate of a correctional institution or under the custody of a law enforcement official, Clay County may disclose PHI to the institution or official for certain purposes including the health and safety of the individual and others.

15. Fundraising Activities. Clay County may use certain information, limited to contact information such as name, address and phone number and the dates of treatment or services, to contact an individual in an effort to raise money for purposes permitted by HIPAA. The individual (or appropriate representative) may opt out of receiving further fundraising communications. A written decision to opt out shall be treated as a revocation of authorization. If an individual has opted out, Clay County will ensure that he/she are not sent such communications by removing his or her name from all fundraising contact information and maintaining his or her name on a "no contact" list.

16. Business Associates/Subcontractors. Clay County may provide some services through "business associates" or subcontractors. Clay County may disclose PHI to such business associates or subcontractors so that they can perform the job Clay County has asked them to do. Clay County will require a business associate or subcontractor to sign a HIPAA-compliant business associate agreement.

17. Family Member Or Others Involved In Care Or Payment. Clay County may disclose, without individual authorization, to a family member, other relative or close personal friend of the individual – or any other person identified by the individual – PHI directly relevant to this person's involvement with the individual's care or payment for that care. The individual shall be provided notice and an opportunity to agree or object or, if the individual is present, Clay County may reasonably infer that the individual does not object to the disclosure. However, if the individual is not present or available Clay County may determine in its professional judgment whether the disclosure is in the individual's best interest.

Other Special Situations

Under HIPAA, special rules apply to certain types of PHI or certain activities, which are further described below.

1. Marketing and Treatment Alternatives and Health-Related Benefits and Services. Clay County may use or disclose PHI to inform about treatment alternatives and health-related benefits and services, so long as Clay County is not directly or indirectly compensated for these communications. To that end, it shall be Clay County's policy to obtain an authorization if PHI is to be used for "marketing", which includes subsidized treatment communications. Marketing shall be defined consistent with the HIPAA regulations. The Privacy Officer will review whether a requested use of PHI constitutes marketing under HIPAA and may consult with legal counsel to make such determination.

2. Psychotherapy Notes. The use and disclosure of psychotherapy notes shall require HIPAA-compliant Authorization except in very limited circumstances permitted under HIPAA, and shall be subject to any applicable state laws which provide greater protection than HIPAA (see Appendix 1 for further requirements under state law).

3. Genetic Information. If Clay County collects or receives genetic information, Clay County will comply with the applicable provisions of the Genetic Information Nondiscrimination Act (GINA) with respect to protecting the privacy of PHI pertaining to genetic information.

4. Information Subject to State Law. State laws that are more stringent than HIPAA shall continue to apply. A state law may be considered more stringent if it provides individuals with greater privacy rights or protections. The attached Appendix I addresses state laws that may be more stringent than HIPAA and/or state laws of which departments should be aware.

SPECIAL RULES FOR MINORS AND PERSONAL REPRESENTATIVES

HIPAA imposes special rules with respect to minors and their personal representatives, which are further described below.

Personal Representatives of Adults and Emancipated Minors

HIPAA requires a covered entity to treat a "personal representative" the same as the individual, with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under HIPAA. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, Clay County shall treat such person as a personal representative, with respect to PHI relevant to such personal representation, subject to narrow exceptions under HIPAA.

Parents and Unemancipated Minors.

In most cases, a parent, guardian, or other person acting *in loco parentis* (collectively, "parent") is the "personal representative" of the minor child and can exercise the minor's rights with respect to PHI, because the parent usually has the authority to make health care decisions about his or her minor child.

However, with respect to PHI, there are three circumstances in which the parent is not the "personal representative" with respect to certain health information about his or her minor child. These exceptions generally track the ability of certain minors to obtain specified health care without parental consent under State or other laws, or standards of professional practice. In these situations, the parent does not control the minor's health care decisions, and thus does not control the PHI related to that care.

The three exceptional circumstances when a parent is not the minor's personal representative are as follows below.

1. When State or other law does not require the consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service.

   Example: A State law provides an adolescent the right to obtain mental health treatment without the consent of his or her parent, and the adolescent consents to such treatment without the parent's consent.

2. When someone other than the parent is authorized by law to consent to the provision of a particular health service to a minor and provides such consent.

   Example: A court may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself.

3. When a parent agrees to a confidential relationship between the minor and a health care provider.

   Example: A physician asks the parent of a 16-year-old if the physician can talk with the child confidentially about a medical condition and the parent agrees.

Regardless, however, of whether a parent is the personal representative of a minor child, State or other applicable laws that expressly address the ability of the parent to obtain health information about the minor child will control. Thus, Clay County may disclose to a parent, or provide the parent with access to, a minor's PHI when and to the extent it is permitted or required by State or other laws (including relevant case law). Likewise, Clay County is prohibited from disclosing a minor child's PHI to a parent, or providing a parent with access to such information, when and to the extent it is prohibited under State or other laws (including relevant case law).

In cases in which State or other applicable law is silent concerning parental access to the minor's PHI, and a parent is not the personal representative of a minor child based on one of the exceptional circumstances described above, Clay County has discretion to provide or deny a parent with access to the minor's health information, if doing so is consistent with State or other applicable law, and provided the decision is made by a licensed health care professional in the exercise of professional judgment.

SPECIAL RULES FOR DECEASED INDIVIDUALS

Except as provided in the "Special Situations" section above, or as permitted or required by HIPAA, the PHI of deceased individuals will be subject to all of the same privacy protections as if the individual were alive. However, there are two exceptions to this general rule, which are further described below.

1. Individuals Involved In Care. If the individual is deceased, Clay County may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to Clay County.

2. Deceased for 50 Years. The health information of an individual who has been deceased for 50 years or longer shall no longer be considered PHI.

VERIFICATION OF IDENTITY

Prior to any disclosure permitted by this subpart, Clay County shall: (i) except with respect to disclosures to family members or others involved in the individual's care, verify the (a) identity of a person requesting PHI and (b) the authority of any such person to have access to PHI, ***if the identity or any such authority of such person is not already known to Clay County***; and (ii) obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the disclosure.

Verification can be completed in one of the following ways as described below.

1. **In-person:** Photo-ID • Driver's License • Passport

2. **Mail**: Signature validation: Compare the signature on the mailed request with the client's signature on file. When the request is to mail records, the records should be sent to the address on file. Requests to send records to someone other than the client must be in writing and properly validated, with client signature.

3. **Phone**: Request full name and at least two other identifiers such as date of birth, address, emergency contact name, phone number, or last 4 digits of their social security number. If doubt persists, call the client back using the phone number listed in the file.

4. **Email:** Address verification: email address must match that provided by the client previously and on file. Requests to send records to someone other than the client must be in writing and properly validated, with client signature.

For persons acting through legal process, it may be necessary to show an applicable warrant, subpoena, order, or other legal process issued by a grand jury or judicial administrative tribunal. The conditions may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met. The documentation may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with HIPAA rules.

Clay County may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official: (i) if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; (ii) if the request is in writing, the request is on the appropriate government letterhead; or (iii) if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

Clay County may rely, if such reliance is reasonable under the circumstances, on either of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official: (i) a written statement of the legal authority under which the information is requested or (ii) if a written statement would be impracticable, an oral statement of such legal authority. If a request is made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

ATTACHMENT:

APPENDIX I – State Privacy and/or Confidentiality Laws
APPENDIX II – Form 1 – Confidentiality Agreement

MINIMUM NECESSARY USES AND DISCLOSURES

Overview of the Minimum Necessary Rule

Clay County will use or disclose only the minimum amount of PHI necessary and appropriate to accomplish the purpose for which the information is sought (i.e., the "minimum necessary" rule).

The minimum necessary requirement does not apply to:

(i) Disclosures to, or requests by, a health care provider for treatment purposes;
(ii) Disclosures to the individual who is the subject of the information;
(iii) Uses or disclosures made pursuant to an individual's authorization;
(iv) Uses or disclosures required for compliance with HIPAA;
(v) Disclosures to HHS when disclosure of information is required under the HIPAA Privacy Rule for enforcement purposes; and
(vi) Uses or disclosures that are required by other law.

Workforce Members will remain diligent in their efforts to comply with the minimum necessary rule when determining appropriate access, use, and disclosure of PHI.

Applying the Minimum Necessary Rule to Access and Uses of PHI

Clay County, its Workforce Members, and Business Associates must make reasonable efforts to limit the amount of information it accesses and uses to the minimum necessary to accomplish the intended purpose for such use or access. Program Leaders are responsible for identifying the Workforce Members or teams within their programs or department who need access to PHI to carry out their duties, and for designating the types of PHI needed by each Workforce Member or group to carry out their work duties.

In certain instances, Clay County may rely on the judgment of the party requesting PHI access that the PHI being requested is the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

(i) A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the HIPAA Privacy Rule, such as for public health purposes (45 CFR 164.512(b)).

(ii) A Covered Entity under the Privacy Rule. Covered entities would include a health plan, a health care provider, or a health plan clearinghouse.

(iii) A professional who is a Workforce Member or Business Associate of Clay County who states that the information requested is the minimum necessary for the stated purpose.

In all other instances, the Privacy Officer shall review and determine whether the access request meets the minimum necessary rule.

Applying the Minimum Necessary Rule to PHI Disclosures

Disclosures of PHI must also adhere to the minimum necessary rule. The requirements needed to meet the minimum necessary rule when disclosing PHI varies slightly based on whether the disclosure is considered "routine and recurring" or "non-routine".

Routine and Recurring Disclosures

"Routine and recurring disclosures" are disclosure of records outside of Clay County without the authorization of the individual or their designated legal representative, for a purpose compatible with the purpose for which the information was collected. These purposes broadly include: (i) disclosures for treatment purposes or payment purposes, (ii) disclosures made to managed care organizations or federal and state agencies for the purpose of audit or oversight, or (iii) disclosures to a state licensing board.

Workforce Members will take the following steps for routine or recurring disclosures:

(i) Confirm that the applicable Clay County policies permit the requested use or disclosure;

(ii) Determine who is requesting the information and the purpose for the request, and confirm that it is compatible with the scope of the request; and

(iii) Identify the kind of information that is necessary to respond to the request consistent with the minimum necessary rule.

Reasonable efforts will be made to limit each PHI user's access to only the PHI that is needed to carry out his/her duties. These efforts will include departmental use of PHI.

Non-routine Uses and Disclosures

"Non-Routine uses and disclosures" are those made outside of Clay County that are not compatible with the purpose for which they are collected. Examples of non-routine disclosures may include: (i) those made in compliance with a court order and (ii) those made to another department or program in order to avert a serious threat to public health or safety and the disclosure is requested by a person who is able to prevent or lessen the threat.

In cases involving non-routine disclosure requests, Workforce Members will (i) apply the steps listed under "routine and recurring disclosures" above to ensure the minimum necessary rule is applied and (ii) have the request reviewed at a supervisory level or above and assessed on an individual basis in accordance with the criteria set forth in this Policy.

Workforce members shall apply the rules below when assessing non-routine requests.

(i) Individual requests for disclosure (i.e., other than an authorization) will be reviewed by medical record staff or a case worker, so that the information disclosed is limited to that which is reasonably necessary to accomplish the purpose for which disclosure is sought. A request may be considered limited to the minimum necessary if the request is from a Clay County official, another covered entity, or a professional for the purpose of providing services to the covered entity, and the request states that the PHI requested is the minimum necessary.

(ii) Requests for disclosure from external non-covered entities will be reviewed to ensure that the response limits the disclosed information to that which is reasonably necessary to accomplish the purpose for which disclosure is sought.

(iii) Outside requests for records (subpoenas/court orders): Any response to outside requests for information on individuals will be responded to by the Privacy Officer.

(iv) Please see Appendix 1 – State Privacy and/or Confidentiality Laws for further requirements under Minnesota law.

Special Rules For the Release of Entire Designated Record Set

In cases of either routine or non-routine disclosures, access to an entire portion of the files containing the designated record set is acceptable as long as the appropriate justification is specifically provided and documented. However, an entire designated record set may not be disclosed unless:

(i) It is authorized in writing by the individual or their designated legal representative; and

(ii) The entire designated record set is specifically justified as the amount of information that is reasonably necessary to accomplish the purpose of the disclosure, and such justification is documented.

AUTHORIZATION TO USE OR DISCLOSE PHI

Clay County requires the use of a valid and complete authorization to use and disclose PHI for reasons other than as permitted under HIPAA (see "Permitted Uses and Disclosures of PHI" above for further information on purposes that do not require authorization). Clay County may not use or disclose information on individuals for any additional purpose without an authorization. Under no circumstances will Clay County require individuals to authorize additional uses and disclosures as a condition or provision of receiving services.

Clay County believes that individuals have the right to know and often times to decide how their PHI will be used. An authorization provides the individual and Workforce Members with details regarding from whom they may obtain PHI, how PHI will be used and to whom PHI may be disclosed. HIPAA grants individuals the right to "revoke" a prior authorization. A "revocation of authorization" allows an individual to withdraw permission given to Clay County regarding the gathering, using, and disclosing of PHI.

For the avoidance of doubt, individuals always have the right to disclose PHI on their own.

Please see Appendix 1 – State Privacy and/or Confidentiality Laws for further requirements under Minnesota law.

Circumstances Where Authorization is Obtained

Authorization forms are typically used when:

(i) When an individual or other entity requests release of an individual's PHI for purposes other than treatment, payment, or health care operations;

(ii) Clay County seeks to obtain verbal and/or written information from another agency, organization, or person; or

(iii) Clay County obtains an "Authorization for Text Messaging" form (see Appendix II, Form 3) for unencrypted text messaging upon intake.

Authorization Requirements

In order to be a valid HIPAA authorization, the requirements described below must be met.

1. Authorizations must be in writing, signed, and dated in ink.

    (a) If an individual has been legally adjudicated as unable to sign legal documents and a legal guardian has been court appointed, then the guardian has the right to consent to disclosure of PHI maintained by Clay County. The legal guardian must provide a certified copy of her/his order of appointment. The individual shall still be advised that disclosure is anticipated.

(b) In cases involving unemancipated minors, the minor's parent or legal guardian must sign the release as well as the minor.

2. The Authorization Form must include the following information:

(a) the name of the person whose PHI will be released;
(b) the signature of the person whose PHI will be released, or the parent or legal guardian of a person who is unable to provide authorization;
(c) the specific PHI to be released;
(d) the purpose for which the PHI is to be used;
(e) the date the authorization takes effect;
(f) the date the authorization expires;
(g) the name of the organization or person to whom the PHI is to be released;
(h) the name of the organization or person within the organization who is providing the PHI;
(i) a statement that the person or family may withdraw their authorization at any time; and
(j) a statement that prohibits re-disclosure of the PHI.

3. All sections of Clay County's "Authorization to Release Information" form (see Appendix II, Form 2)[1] must be completed prior to obtaining the signature of the individual. Under no circumstances should an individual be asked to sign a blank or incomplete Authorization.

4. A copy of the signed "Authorization to Release Information" form shall be given to the individual or legal representative when Clay County requested the authorization; otherwise upon request. A copy of the "Authorization to Release Information" form shall also be placed in the consent section of the person's files.

5. A signed authorization must never be used as a condition to receive services. Services will never be denied because an individual chooses not to sign an "Authorization to Release Information" form.

Defective Authorization

An authorization is not valid if the document has any of the following defects:

(i) The expiration date has passed, or the expiration event is known by Clay County to have passed;

[1] *DHS has translated the "Authorization for Release of Information" portion of this release of information into Arabic, Hmong, Lao, Oromo, Russian, Serbo-Croatian, Somali, Spanish and Vietnamese. When requesting a client signature on this release form from a client with limited proficiency, attach a copy of the appropriate translation of the consent portion to the English form for the client to review before signing. The client will sign the English version since that is what is sent to the person/organization providing the information).*

(ii) The authorization has not been filled out completely, i.e., one of the elements noted above under "valid authorization" is missing or not completed;

(iii) Clay County knows that the authorization has been revoked;

(iv) Clay County knows that any material information in the authorization is false; and/or

(v) The authorization is a prohibited "compound authorization", which means that the authorization was combined with another document, including any other written legal permission from the individual or the individual's representative.

Documentation

Clay County Workforce Members must document and retain all signed authorizations in the individual's medical record.

Revocation of an Authorization

The following steps below must be applied to revoke authorization.

1. Individuals must submit requests to revoke an authorization in writing ("Revocation of Authorization"). The individual or legal representative must sign and date the revocation.

2. The Workforce Member will inform the individual or legal representative that the revocation of an authorization stops further uses and disclosures of their health information that were allowed pursuant to the original authorization.

3. The completed and signed revocation will be placed in the individual's files.

Requests for Disclosures from Other Providers

1. Clay County may disclose PHI when a HIPAA compliant authorization is received. HIPAA compliant authorizations contain all of the information required in Clay County's authorization forms (see above).

2. Clay County will deny the request for information if the authorization is not HIPAA compliant.

3. If the authorization is not HIPAA compliant, the agency, organization or person will be notified in writing.

ATTACHMENT:

APPENDIX II – Form 2 – Authorization to Release Information
APPENDIX II – Form 3 – Authorization for Text Messaging

INDIVIDUAL RIGHTS – NOTICE OF PRIVACY PRACTICES

A HIPAA compliant Notice of Privacy Practices ("Notice") (see Appendix II, Form 5) must be given to every individual receiving services from Clay County. Please see Appendix 1 – State Privacy and/or Confidentiality Laws for further requirements under Minnesota law.

Content of the Notice.

The Notice must be written in plain language and contain information on:

(i) How Clay County uses PHI;

(ii) When Clay County may disclose PHI;

(iii) The rights of individuals with respect to PHI;

(iv) Statements required under HIPAA (as further described below);

(v) Clay County's legal duties with regard to PHI; and

(vi) Any other requirements contained in HIPAA, as well as other state and federal laws that impact Clay County's privacy practices.

Required Statements

The Notice of Privacy Practices must contain certain statements as described below.

1. The Notice must include a statement indicating that the following uses and disclosures will be made only with an individual's written authorization:

   (a) Uses and disclosures of psychotherapy notes that are not for permitted treatment, payment, or health care operations;

   (b) Uses and disclosures of PHI for marketing purposes; and

   (c) Disclosures that constitute a sale of PHI.

2. The Notice of Privacy Practices must also contain a statement indicating that Clay County is required to notify the individual of any Breach of his or her unsecured PHI.

3. If Clay County intends to send fundraising communications to the individual, the Notice must inform the individual of the same, and that he/she has a right to opt out of such fundraising communications with each solicitation.

Notice Review and Approval Process.

The Notice must be approved by the Privacy Officer. The Privacy Officer is responsible for revising the Notice to reflect any changes in practices regarding PHI, including material changes to uses or disclosures of PHI, the individual's rights, Clay County's legal duties, or other privacy practices stated in the Notice.

Providing the Notice to Individuals.

Program Leaders are responsible for ensuring that the Notice, or a summary of the same, is posted in a prominent location accessible to individuals. The complete Notice must be made readily available to individuals at each service delivery site for individuals to take with them upon request. The Notice will also be available electronically through Clay County's website.

Workforce Members must provide a copy of the Notice to individuals at the time of the first service delivery. If treatment is first rendered in an emergency, the Notice is given as soon as reasonably practicable after resolution of the emergency.

The Workforce Member giving the Notice shall ask the individual to sign a written acknowledgement of receipt via the "Privacy Notice Acknowledgement and Consent form" (see Appendix II, Form 4). If the individual refuses or is unable to sign, the circumstances will be documented on the Privacy Notice Acknowledgement and Consent form.

Documentation.

The Privacy Notice Acknowledgement and Consent form will be retained in the individual's record for six (6) years. Copies of prior versions of the Notice must also be retained for six (6) years.

ATTACHMENTS:

APPENDIX II – Form 4 – Privacy Notice Acknowledgement and Consent
APPENDIX II – Form 5 – Notice of Privacy Practices

INDIVIDUAL RIGHTS – RIGHT TO ACCESS PHI

Policy

Individuals and their designated legal representatives shall have access to their PHI, consistent with HIPAA and all applicable federal and state law and regulations and supported by Clay County's professional judgment as to the best interest of the individual. Please note that state privacy laws may impose additional requirements beyond what is enumerated under HIPAA. Please see the "Minnesota Government Data Practices Act (MGDPA), Individual Rights" section within Appendix 1 - State Privacy and/or Confidentiality Laws for further requirements that may go beyond HIPAA. Please also refer to the Bill of Rights Policy and Data Practices Policies for further rules regarding data access requests.

Right to Access

Subject to certain exceptions noted below, HIPAA grants individuals the right to access their own PHI in a Covered Entity's Designated Record Set for the purpose of inspecting and/or copying that information. Information in a Designated Record Set includes all records maintained by Clay County related to an individual's payment or treatment and may include records related to audits of claims for quality review purposes.

Clay County will provide access to the individual's PHI without regard to whether it created the information unless the information is subject to one of the conditions for denial of access. (See "Exceptions to the Right of Access" and "Denials to Right of Access" below). Clay County will provide access to information for as long as the records are maintained by Clay County.

An individual is not required to make a separate request to each originating provider. Program Leaders will work with the Privacy Officer in appropriate circumstances. If Clay County does not maintain and cannot access the information that is sought by the individual, but Clay County knows where the information is maintained, Clay County will inform the individual where to direct the request for access. In addition to providing access to information already in its possession, Clay County will provide access to information, which is held in the records of a subcontractor, pursuant to its Business Associate Agreement, unless the information is the same as the information maintained by Clay County.

Exceptions to the Right to Access

An individual does not have a right to access to the following information:

(i) Psychotherapy notes (however, please see Appendix 1);
(ii) Information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and

(iii) laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories.

Denials to Right to Access

There are instances in which Clay County may deny an individual's request for access. Clay County should exclude only that information that is subject to a denial and allow access to other information.

Denials fall into the following two general categories, depending upon whether the denials are subject to further review.

1. Denials which are not subject to further review

In certain limited instances, Clay County may deny an individual's access to information without providing the individual with an opportunity to have that denial reviewed.

These instances include the following:

(a) PHI which falls into one of the enumerated exceptions in the "Exceptions to the Right to Access" section above;

(b) PHI requested by an inmate of a correctional institution which Clay County has been directed by the correctional institution to deny, as obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or of any officer, employee, or other person at the correctional institution or responsible for transporting the inmate (if the inmate requests inspection of the PHI, the request must be granted unless one of the other grounds for denial applies);

(c) PHI is created or obtained in the course of research that includes treatment, as long as the individual has agreed to a denial of access at the time of consenting to participate in the research (this denial of access is allowed only for as long as the research is in progress – once the research is concluded, the individual's right of access is reinstated.

(d) PHI is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, if the denial of access under the Privacy Act would meet the requirements of that law; and

(e) Information obtained from someone else, other than a health care provider, that was obtained under a promise of confidentiality, but only if access would be reasonably likely to reveal the source of the information.

2. Denials that require further review

In other instances, Clay County may deny an individual access to information, provided that the individual is given a right to have the denial reviewed. If access is denied in these instances, the individual has the right to request a review of the denial by a licensed health care professional who is designated by Clay County to act as a reviewing official and who did not participate in the original denial. Once the reviewing official issues a determination, Clay County must act in accordance with that determination. Denials that provide a right of further review include the following:

(a) Denial of access to PHI which, upon a determination of a licensed health care professional, is reasonably likely to endanger the life or physical safety of the individual or another person;

(b) Denial of access to PHI which makes reference to another person (other than a health care provider) and which, upon a determination of a licensed health care professional, is reasonably likely to cause substantial harm to that other person; or

(c) Denial of access to PHI requested by an individual's personal representative which, upon a determination of a licensed health care professional, is reasonably likely to cause substantial harm to the individual or another person.

Procedure

1. Individuals will be notified of their right to receive copies of their PHI records in the designated record set through the Notice of Privacy Practices.

2. Applicable Program Leaders and/or the Privacy Officer will be responsible for receiving and processing requests for access

3. *Requesting Onsite Review of an Individual's PHI Record*

(a) An individual wishing to review his or her file must make a written request for this to his or her Clay County point of contact, which may be a social worker or team leader ("client contact").

(b) The client contact will then arrange for a time and place for the individual to review the file. This appointment will be arranged within 10 business days of the request.

(c) An appointment to review the file at Clay County headquarters will then be arranged during regular business hours.

(d) A Clay County Workforce Member will be available to help the consumer with any problems that may arise in reviewing the file.

4. *Requesting a Copy of the Individual's PHI Record*

(a) Individuals must request copies of their PHI records, in writing, to the appropriate contact for processing by using the "Request for Information Minnesota Government Data Practices Act form" (see Appendix II Form 6), which is available on Clay County's website or from the Privacy Officer.

(b) Upon verification of the individual's legal authority to access and receive copies of the PHI records, the applicable Workforce Member will review and copy the PHI record. A copy of the "Request Form for Copies of an individual's Records" must be sent to the Privacy Officer for HIPAA monitoring purposes. Please see the "Permitted Uses and Disclosures" Section of the Policy for further information on proper verification procedures.

4. *Providing Copies of PHI Records*

(a) Timing of Request. Clay County shall address the access request, within 10 calendar days of receiving the written request.

(b) Format of PHI Records. Clay County will provide access to PHI in the form or format requested by the individual if it is readily producible in that form or format. If the information is not in the form or format requested by the individual, then Clay County will provide the PHI in a readable hard copy form or other form or format that has been agreed to between the individual and Clay County. Clay County may provide the individual with a summary or explanation of the information if the individual has agreed, in advance, to such a summary or explanation and to any fees that may be imposed as a result of providing such a summary or explanation. When an Electronic Health Record exists, Clay County, including a subcontractor, must comply with a request for access to the record in electronic format, and/or must comply with a request to transmit an electronic record directly to an entity or person directed by the individual.

(c) Content of PHI Records. The PHI record provided to individuals shall contain the following information:

(i) The individual's name on each page of the record.
(ii) The date on which the entry is made.
(iii) The date the service is provided.
(iv) The length of time spent with the individual.
(v) The signature and title of the person providing the service.
(vi) Documentation of the individual's progress toward goals and changes in treatment or diagnosis.
(vii) Documentation of supervision by the supervisor.

(viii) The individual's case history.
(ix) All assessments.
(x) Diagnostics.
(xi) Reports of consultations ordered for the individual.
(xii) Individual treatment plan.
(xiii) Physician's orders.
(xiv) Laboratory reports.

(d) Provision of PHI Records. Clay County will provide access to information in a timely manner and at a mutually convenient date, time and place for inspection and copying of the information, including mailing a copy of the information if the individual so requests. The individual will be given the opportunity to have the copies of the PHI records mailed at the individual's cost, or to come to the Clay County facilities to pick up the records personally (or may select another manner of receipt).

(i) *In Person Pickup.* When records are picked up in person the following process must be applied:

1. The individual must provide two (2) forms of identification, one of which must be a photo-identification unless there are ethnic or religious prohibitions to photographic images. If there are ethnic or religious prohibitions to photographic images, the individual may substitute another form of identification. The forms of identification will be indicated on the receipt form.

2. The individual picking up the PHI records must sign a "Receipt Form for Copies of Client/Customer Records" (see Appendix II, Form 7), indicating that they took delivery of the copied records.

(ii) *Mailed Requests.* When it is requested that records be mailed, records will only be sent "Return Receipt Required." A "Receipt Form for Copies of Client/Customer Records" will be sent with the record with instructions for the requestor to sign and return.

(iii) A copy of the filled-out "Receipt Form for Copies of Client/Customer Records" must be sent to the Privacy Officer.

(e) Providing of a Denial Response. In denying access, Clay County should consider the reasons for denial set forth above under the subsection entitled "Denials to Right of Access". If Clay County makes a determination to deny access, Clay County must provide to the individual a written notice of denial drafted in plain English and must contain:

(i) The basis for denial;

(ii) If the denial is subject to further review, a statement of the individual's rights to have the denial reviewed and a description of how the individual may exercise those rights; and

(iii) A description of how the individual may submit a complaint to the Clay County General Privacy Officer or to the Secretary of the Department of Health and Human Services using the complaint processes set out in other sections of the rule.

A copy of the written denial must be provided to the Privacy Officer for his/her records.

(f) Addressing an Individual's Request to Review a Denial Decision. Requests for a review of a denial decision will be submitted to the Privacy Officer.

The Privacy Officer will:

(i) Designate a licensed health care professional not directly involved in the denial to review the decision to deny;

(ii) Promptly refer the individual's request for review to the designated reviewing official;

(iii) Ensure that the designated reviewing official issues a determination within a reasonable period of time regarding whether to uphold or overturn the denial;

(iv) Upon receipt of the reviewing official's determination, promptly notify the individual, in writing, of the determination; and

(v) Take action in accordance with the reviewing the official's determination.

(g) Costs. Clay County may impose reasonable, cost-based fees for any of the following:

(i) Copying, including the cost of supplies for and labor of copying;

(ii) Preparation of an explanation or summary of the information, provided that the individual has agreed in advance to such costs; and

(iii) Postage, when the individual has requested a copy, or a summary or explanation, to be mailed.

Costs may be limited based on applicable Minnesota law. No fees can be charged to recipients of public assistance.

ATTACHMENTS:
APPENDIX II – Form 6 – Request Form, Copies of Individual's PHI Records
APPENDIX II – Form 7 – Receipt Form, Copies of Individual's PHI Records

INDIVIDUAL RIGHTS – RIGHT TO REQUEST AN AMENDMENT TO PHI

Policy

Individuals who receive services from Clay County have the right to request that Clay County amend PHI about them in Clay County's records as long as the PHI is maintained by Clay County. It is Clay County's policy to respond to an individual's request for an amendment to his or her PHI held by Clay County and/or our Business Associates in compliance with HIPAA and applicable state laws.

Please note that state privacy laws may impose additional requirements beyond what is enumerated under HIPAA. Please see the "Minnesota Government Data Practices Act (MGDPA), Individual Rights" section within Appendix 1 - State Privacy and/or Confidentiality Laws for further requirements that may go beyond HIPAA.

Please also refer to the Clay County Data Practices Policies for further rules regarding individual requests to amend PHI.

While an individual has the right to request an amendment, Clay County does not have an absolute obligation to grant that request and may deny the request to amend in the following instances:

(i) Upon a determination by Clay County that the information sought to be amended was not created by Clay County, unless the individual provides a reasonable basis of belief that the originator of the information is no longer available to act on the request;

(ii) The information sought to be amended is not a part of a Designated Record Set;

(iii) The information sought to be amended is not available for inspection under one of the exceptions or pursuant to one of the non-reviewable denials identified in Clay County's "Right to Access PHI" policy above; or

(iv) The information sought to be amended is accurate and complete.

Procedure

1. *Request Submission.* Individuals and their legal representatives must submit their request to amend their PHI in writing on Clay County's "Request Form, Amendment of PHI Records" (see Appendix II, Form 8). Individuals can obtain the "Request Form, Amendment of an Individual's PHI Records" on Clay County's website or by contacting the Privacy Officer.

2. *Request Review.* The Workforce Member who receives the request must date stamp the request and forward the request to the applicable program or department for review. The reviewer will:

(a) Forward a copy of the request to the Privacy Officer;

(b) Coordinate a review of the record by the appropriate department or program;

(c) Ensure the review is documented; and

(d) Determine whether to grant or deny the request for amendment.

3. *Timing of Response.* Clay County will respond to a request to amend records within 30 days of receiving the request.

4. *Acceptance of the Request.* If Clay County decides to grant the request, either in whole or in part, Clay County or its designee must do the following:

(a) Inform the individual, in writing, that the amendment request is accepted;

(b) Obtain the individual's identification and agreement to have Clay County notify the relevant persons with which the amendment needs to be shared, including Clay County's Business Associates;

(c) Identify the records in the Designated Record Set that are affected by the amendment and then append or otherwise provide a link to the location of the amendment; and

(d) Log the result and how the record will be changed on an internal memo.

5. *Denial of the Request.* If Clay County decides to deny the request, Clay County or its designee must provide the individual with a timely, written notice of denial in plain language. The denial must include the following information:

(a) The basis for denial;

(b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(c) A statement that, if the individual does not submit a statement of disagreement, the individual may request that Clay County include the request for amendment and the denial in any future disclosures of the information that is the subject of the requested amendment; and

(d) A description of how the individual may submit a complaint to Clay County using Clay County's complaint and/or grievance process or to the Department of Health and Human Services, Office of Civil Rights. This description must include the name, or title, and telephone number of the contact person or office who is responsible for the receipt and processing of such amendment requests.

6. *Statement of Disagreement.* If an individual submits a statement of disagreement, Clay County will include the documentation identified above, or a summary of such documentation if the individual agrees in advance, with any subsequent disclosure of the information. Clay County has a right to submit a written rebuttal to the individual's statement of disagreement, and must provide a copy of its rebuttal to the individual. If the individual has submitted a statement of disagreement, Clay County must include the material appended, or an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates. If an individual does not submit a statement of disagreement, then Clay County will include the individual's request and the denial (or an accurate summary) with any future disclosure of the information, but only if the individual has requested such action. If Clay County is informed by another covered entity of an amendment to an individual's PHI, Clay County will amend the PHI in designated record sets. Amendments will be made in a reasonable time period as expeditiously as possible.

7. *Documentation.* Workforce Members must provide to the Privacy Officer copies of the following documentation:

   (a) The record(s) that are the subject of the requested amendment, including any amendment made to those records;

   (b) The individual's request for amendment;

   (c) The written response to the request for amendment;

   (d) The individual's statement of disagreement, if any;

   (e) Clay County's rebuttal, if any; and

   (f) The titles of the persons or offices responsible for receiving and processing amendment requests.

8. *Retention.* The individual's written request will become a part of any case file maintained on the individual. All requests to amend documentation will be retained in accordance with the County's approved General Records Retention Schedule.

ATTACHMENT:
APPENDIX II – Form 8 – Request Form, Amendment of an Individual's PHI Records

INDIVIDUAL RIGHTS – RIGHT TO ACCOUNTING OF DISCLOSURES OF PHI

Policy

Overview

At the request of an individual, Clay County will provide a list of an accounting of disclosures of PHI made by Clay County in the six years prior to the date on which the accounting is requested as required by law, excluding disclosures made:

(i) To carry out treatment, payment, and health care operations;

(ii) To an individual regarding their own information;

(iii) For the agency's directory or to persons involved in the individual's care;

(iv) For national security or intelligence purposes;

(v) To correctional institutions or law enforcement officials;

(vi) That occurred prior to April 14, 2003; or

(vii) That occurred pursuant to an Authorization.

Temporary Suspension of an Individual's Right to Receive an Accounting

1. Written Notice of Suspension by Government Agency/Official.

   Clay County must temporarily suspend an individual's right to receive an accounting of disclosures if a health oversight agency or law enforcement official, in a written statement, informs Clay County that such an accounting would be reasonably likely to impede the agency's activities. The written statement must specify the time period for which the suspension is required.

2. Oral Notice of Suspension by Government Agency/Official.

   If a health care agency or law enforcement official provides Clay County with oral notice of the need to suspend an individual's right to receive an accounting, then Clay County will:

   (a) Document the oral statement, including the identity of the agency or official making the statement;

   (b) Temporarily suspend the individual's right to an accounting; and

(c) Limit the suspension to no longer than 30 days from the date of the oral statement, unless the agency or official provides Clay County with a written statement as set forth above.

Procedure

1. *Request for an Accounting.* Individuals and their legal representatives must submit their request for an accounting of disclosures of PHI in writing on using the "Request for an Accounting of Disclosures of Health Information" form (see Appendix II, Form 9), which is available on the Clay County website or may be obtained from the Privacy Officer.

2. *Receipt of Form.* Upon receipt of a Request for an Accounting of Disclosures of Health Information, the Clay County shall review the form and determine whether all information necessary to respond to the request has been provided. If the form has not been completed correctly or information is missing, the Clay County will take whatever steps are deemed necessary to complete the form, including returning the form to the requestor with an explanation. If the form has been completed correctly and completely, the Clay County shall compile the accounting of disclosures in accordance with the remainder of this policy and procedure.

3. *Submission to the Privacy Officer.* The Workforce Member who receives the request must date stamp the request and forward the request to the Privacy Officer for review.

4. *Request Review.* The Privacy Officer or her/his designee will review the files of the individual for documentation of disclosures for which an accounting may be prepared. These include disclosures to and by Business Associates.

5. *Timing of Response*. The Privacy Officer or her/his designee will respond to a request for an accounting of disclosures within 60 days of receiving the request. If Clay County is unable to act on the request within the time period specified above, Clay County may extend the time by no more than 30 days, but only if:

   (a) Clay County notifies the individual in writing that it is unable to act on the request within the allowed time period, stating the reasons for the delay and the date by which Clay County will respond to the request; and

   (b) Clay County has taken no other extensions of time with regard to this particular request.

6. *Content of Response.* The accounting of disclosures provided to the individual will be in writing and will include:

   (a) Disclosures of information that occurred during the 6 years prior to the date of the request (or a shorter time period as requested by the individual);

(b) Disclosures made to or by Clay County's Business Associate(s);

(c) The dates of each disclosure;

(d) The name (and address, if known) of the entity or person who received the information;

(e) A brief description of the information disclosed;

(f) A brief statement of the purpose for the disclosure (or, in lieu of such statement, a copy of a written request for disclosure); and

(g) For multiple disclosures made during an accounting period to the same person or entity for a single purpose or pursuant to a single authorization Clay County's response also must include:

(i) The frequency, periodicity, or number of disclosures made during the accounting period, and

(ii) The date of the last such disclosure.

7. *Cost.* Clay County will provide the first accounting to an individual, in any 12-month period, without charge. Thereafter, for any additional accounting requested within that same 12- month period, Clay County will charge a reasonable, cost-based fee. Clay County will provide advance notification of the fee to the individual so as to provide the individual with an opportunity to withdraw or modify the request.

Responsibilities of the Privacy Officer

The Privacy Officer shall be responsible for overseeing the implementation of the steps in this policy and procedure, including the following:

(i) Ensuring that the Notice of Information Privacy Practices, if applicable, adequately discusses an individual's right to request an accounting of disclosures.

(ii) Designing and updating, as appropriate, the Request for an Accounting of Disclosures of Health Information form, as well as any standard forms developed to be used for the accounting.

(iii) Reviewing any requests for an accounting of disclosures and responding in the required time frames.

(iv) Notifying the senior leadership of any requests that he/she receives for an accounting of disclosures of health information.

(v) Maintaining a copy of all accountings that are prepared by Clay County.

ATTACHMENT:

APPENDIX II – Form 9 – Requests for an Accounting of Disclosures of Health Information

INDIVIDUAL RIGHTS – RIGHT TO REQUEST RESTRICTION ON USE AND DISCLOSURE OF PHI

Policy

Overview of Restriction Right

Clay County recognizes the right of an individual and their legal representative to request restriction on uses and disclosures of PHI and will make an informed decision regarding whether or not this request can be granted.

An individual has a right to request that Clay County restrict the use or disclosure of PHI as follows:

(i) Restriction on the uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations.

(ii) Restriction on disclosures made to an individual's family, friends, or relatives.

(iii) Restriction on disclosure of PHI for all purposes other than treatment if the individual pays Clay County out-of-pocket in full for the health care services.

Clay County is not required to agree to a request for restriction, except for the restriction contained in (iii) above. In some instances, Clay County may determine, in consultation with the individual, that it is proper to restrict the use or disclosure of certain PHI, while denying restriction on the use or disclosure of other PHI.

If Clay County agrees to a restriction, Clay County may not use or disclose information in violation of that agreement to restrict, except in accordance with the following conditions:

(i) A use or disclosure of restricted information may be made by Clay County for purposes of providing treatment to an individual in the event of an emergency medical condition; and

(ii) If restricted information is disclosed to another health care provider during the course of providing emergency treatment, Clay County must request that the health care provider not further use or disclose the information.

Exceptions

An agreement to restrict the use and disclosure of information does not prevent uses or disclosures made for the following purposes:

(i) For disclosures to the individual;

(ii) For the purpose of inclusion in a facility directory;

(iii) In the event of emergency situations;

(iv) As required by law;

(v) For the purpose of certain public health activities;

(vi) For the purposes of reporting information to law enforcement officials or state agencies about victims of abuse, neglect, domestic violence, or other crimes;

(vii) For the purpose of health agency oversight activities or law enforcement investigations;

(viii) For the purpose of judicial or administrative proceedings;

(ix) For the purpose of identifying decedents to coroners and medical examiners, including determining a cause of death;

(x) For the purposes of organ procurement;

(xi) For certain research activities; and

(xii) For worker's compensation programs.

Third Parties

Clay County may inform others of the existence of a restriction, when appropriate, so long as it does not amount to a *de facto* disclosure of the restricted PHI.

A restriction that is agreed to between an individual and Clay County is only binding on Clay County and not on downstream entities. However, any Business Associate(s) of Clay County are bound by the restriction since a Business Associate cannot use or disclose PHI in any manner that Clay County would not be permitted to use or disclose such PHI.

Procedure

1. *Request for Restriction.* Individuals and their legal representatives must submit their request for restriction on use or disclosure of PHI in writing on Clay County's "Restriction on use of PHI and Disclosure" form (see Appendix II, Form 10), which is available on Clay County's website or may be obtained from the Privacy Officer.

2. *Receipt of Request.* The Workforce Member who receives the request must date stamp the request and forward the request to the applicable Program Leader for

review. The Program Leader will forward a copy of the request to the Privacy Officer.

3. *Determination.* The Privacy Officer will consult with the appropriate Program Leader, as needed, to determine whether or not Clay County will agree with the requested restriction.

4. *Response.* The Privacy Officer will communicate the decision to the individual or their designated legal representative in writing and will send a copy of the communication to the treatment team.

5. *Documentation.* The original request will be placed in the files of the individual. A copy of the request and all attached documentation will be maintained by the Privacy Officer. A copy of the request may also be maintained in a centralized location by clerical Workforce Members for the reporting and processing of such restrictions.

6. *Termination by Clay County.* Clay County may terminate its agreement to restrict the uses and disclosures of an individual's information under the following conditions:

   (a) If the individual agrees to or requests the termination in writing;

   (b) If the individual orally agrees to the termination and the oral agreement is documented; or

   (c) If Clay County informs the individual or their legal representative that it is terminating the agreement. Any PHI created and received after the termination will not be restricted. However, any PHI created or received before termination will be restricted.

7. *Termination by the Individual.* If the individual sends a request to terminate the restriction agreement, the Workforce Member who receives the request to terminate the restriction must document the request and forward the request to the Privacy Officer. The Privacy Officer will provide written notification to the individual or their designated legal representative that the termination of restriction has been received and will send a copy of the notification to the Program Leader. The Privacy Officer will document the termination notification as follows:

   (a) A copy of the termination notification will be placed in the files of the individual.

   (b) A copy of the termination notification and all attached documentation will be maintained by the Privacy Officer.

8. *Termination to Avert Harm.* In the event Clay County reasonably believes that disclosure of restricted information is necessary to avert harm (and an emergency condition does not exist), Clay County must ask the individual for permission to terminate or modify the restriction. If the individual does not agree to terminate or

modify the restriction, Clay County must continue to honor the restriction with respect to information created or received subject to the restriction.

ATTACHMENT:
APPENDIX II – Form 10 – Request Form – Restriction on use of PHI and Disclosure

INDIVIDUAL RIGHTS – RIGHT TO REQUEST RESTRICTION ON THE MANNER AND METHOD OF CONFIDENTIAL COMMUNICATIONS

Policy

Clay County will permit individuals to request communication of PHI by alternative means or alternative locations. Clay County may ask for a reason for the request, but Clay County cannot require a reason be provided as a condition for agreeing to confidential communications request.

Clay County may condition its agreement to restrict the manner and method of confidential communication upon the following:

(i) Receipt of information as to how payment for services, if any, will be handled; and

(ii) Specification of an alternative address or other method of contact.

Procedure

1. *Request for Confidential Communications.* Individuals and their legal representatives must submit their request for communication by alternative means or location in writing on Clay County's "Restriction on Manner and Method of Communication of PHI**"** form (see Appendix II, Form 11), which is available on Clay County's website or may be obtained from the Privacy Officer. The request should clearly state that disclosure of all or part of that information could endanger the individual.

2. *Receipt of Request.* The Workforce Member who receives the request must date stamp the request and forward the request to the Privacy Officer.

3. *Determination.* The Privacy Officer will consult with appropriate Program Leaders to determine whether or not Clay County will agree with the request for communication by alternative means and/or communication at an alternative location.

4. *Response.* The Privacy Officer will communicate the decision to the individual or their designated legal representative in writing and will send a copy of the communication to the treatment team and the Program Leader. The communication will include the terms of the restriction, including a description of the alternative means and/or alternative location for contact.

5. *Documentation.* The original request will be placed in the files of the individual. A copy of the request and all attached documentation will be maintained by the Privacy Officer. A copy of the request may also be maintained in a centralized location by clerical Workforce Members for the reporting and processing of such restrictions. Clay County will maintain requests for alternative means of communication and any

denials of such request in the records of individuals for six years.

6. *Implementation.* Program Leaders are responsible for ensuring:

   (a) that agreed upon alternative means of communication are communicated to applicable Workforce Members and Business Associates who may be sending the individual confidential communications; and

   (b) that when communication by alternative means is granted, the alternative means are clearly indicated on the paper and/or electronic record of the individual.

ATTACHMENT:

APPENDIX II – Form 11 – Request Form, Restriction on Manner and Method of Communication of PHI

INDIVIDUAL RIGHTS – RIGHT TO FILE A PRIVACY COMPLAINT

Policy

Individuals and their legal representatives have the right to file a complaint with Clay County regarding their HIPAA rights in order to seek resolution. Individuals and their legal representatives also have a right to file a complaint with OCR and, to the extent applicable, other governmental bodies.

It is Clay County's policy to keep a record of all complaints and to investigate all complaints to determine the circumstances surrounding any concerns our clients raise regarding privacy. If an individual's privacy rights have been infringed upon in any way, or there is evidence that a Clay County Workforce Member or Business Associate has not adhered to the privacy standards or our policies and procedures, Clay County will take actions consistent with the "Sanctions / Discipline for Violations of HIPAA" section of this Policy and document these actions accordingly.

Under no circumstances will the fact that an individual has filed a complaint with Clay County or with OCR affect the services provided to that individual. Any Workforce Member or Business Associate found to treat any individual differently in light of a complaint will be sanctioned. Any retaliation is prohibited by law.

Procedure

Clay County promotes the resolution of HIPAA issues internally, when possible, by following the steps outlined below.

1. *Complaint Submission.* The individual should submit their complaint in writing and contain information about the concern, such as name, address, phone number and/or email address of contact, along with location, date, and description of the concern. Alternative means of filing complaints, such as personal interviews or a tape recording of the complaint are acceptable alternatives for persons with disabilities, when requested. The individual may use the "HIPAA Complaint" form (see Appendix II, Form 12) to submit his or her compliant, which is which is available on Clay County's website or may be obtained from the Privacy Officer.

2. *Timing of Response.* The Privacy Officer shall address the complaint as soon as possible, but no later than 60 calendar days after receipt of the complaint. If more time is needed to review and investigate the complaint, the Privacy Officer will, within said 60 days, notify the participant, in writing of the delay, and inform the participant of the expected time frame for completion of the review.

3. *Investigation of the Complaint.* The Privacy Officer will conduct an investigation of the complaint, including conducting interviews of appropriate Workforce Members and/or Business Associates, where necessary.

4. *Responding to the Complaint.* Based on the findings from the investigation, the Privacy Officer will determine if there is cause to believe that a violation of HIPAA or this Policy has occurred.

   (a) If no violation has occurred, the findings will be date-stamped, the complaint will be considered closed, and the Privacy Officer will provide written notice of the findings to the individual.

   (b) If cause exists to believe that a violation has occurred, the Privacy Officer will (a) notify the individual of its findings and the intended resolution to the complaint and (b) complete required actions to address the violation. Please see the "Addressing the Violation" section below for further information on how the Privacy Officer shall address the violation.

5. *Complaint Resolution*. Once the complaint has been addressed, the Privacy Officer will complete the "HIPAA Complaint Resolution Checklist" (see Appendix II, Form 13) to document how the complaint was resolved. Where applicable, the original complaint form and HIPAA Complaint Resolution Checklist will be placed in the files of the individual and in the Privacy Officer's files.

6. *Appeal.* If the individual disagrees with the Privacy Officer's decision, the individual may request that the complaint be reviewed. The Privacy Officer will provide the individual with the Minnesota Ombudsman Office contact information or the appropriate state level resource for the particular complaint or concern when appropriate.

7. *Documentation.* All documents relating to complaints will be maintained in a retrievable manner for a minimum of six (6) years.

Addressing the Violation

If the Privacy Officer has determined that a HIPAA violation has occurred, the Privacy Officer will (i) determine which of the following actions below, if any, need to be completed to address the violation and (ii) ensure that any required actions be completed in a timely manner.

To the extent necessary the Privacy Officer shall:

1. Notify any affected parties of the violation to mitigate any harmful effects caused by the violation. Any such notification will be filed in the individual's and Privacy Officer's files;

2. Update and/or implement refresher training to applicable Workforce Members;

3. Review and, if necessary, update Clay County's HIPAA policies and procedures;

4. If warranted, recommend to the appropriate Program Leader that disciplinary action should be initiated against any Workforce Member involved in the violation, after following appropriate Clay County Sanctions Policy including involvement of appropriate personnel; and

5. Notify the appropriate Program Leader of any required actions that need to be completed.

ATTACHMENTS:
APPENDIX II – Form 12 – HIPAA Complaint Form
APPENDIX II – Form 13 – HIPAA Complaint Resolution Checklist

RETENTION OF RECORDS

All records indicated below will be retained by Clay County, either in written or electronic form, for a minimum of six (6) years from either the date the record was created or the date the record was last in effect, whichever is later. Please see Appendix 1 – State Privacy and/or Confidentiality Laws for further requirements under Minnesota law.

1. Policies and procedures on PHI uses and disclosures.

2. Minimum necessary policies and procedures.

3. All signed authorizations.

4. Documentation regarding individual rights, including the policies and procedures for inspection and copying and amendment of PHI, requests for access and amendment and response, and documentation of any agreed-upon restrictions on the use or disclosures of PHI requested by an individual.

5. Records of PHI disclosures for purposes other than payment, treatment, and health care operations.

6. All individual complaints and their outcomes.

7. Records of any sanctions imposed on Workforce Members, agents, contractors, or Business Associates for breach of the privacy rules.

8. Records on any PHI used or disclosed for research purposes.

9. Business Associate Agreements.

10. Documentation that workforce training has been provided.

Records will be held for longer periods of time if required under other applicable laws or Clay County's record retention policies, including the County Human Services General Records Retention Schedule.

PURPOSE & SCOPE

This HIPAA Security Policy ("Policy") applies to the protection of ePHI as required under the HIPAA Security Rule and does not address the requirements under the HIPAA Privacy Rule or other privacy, security, or breach notifications requirements under other local, state, or federal law. It does not apply to any systems or applications not within the control of Clay County ("Clay County"), which may have their own obligations to protect ePHI as required by HIPAA. For the avoidance of doubt, no third-party rights are intended to be created by this Policy. Additional data security requirements under the Disaster Recovery Plan, the FTI and SSA Safeguarding Requirements Policy, Clay County's Acceptable Use Policy, and the Data Practices Policies shall be adhered to and shall be incorporated into this Policy.

For the avoidance of doubt, the security measures outlined herein shall apply to all Clay County Systems and Devices that may hold, transmit, or access personally identifiable information even if such personal identifiable information is not classified as PHI under HIPAA.

SECURITY OFFICER

The Security Officer or its designee which may include the Privacy Officer is responsible for the development and implementation of the Clay County's policies and procedures relating to administrative, physical, and technical measures required under the HIPAA Security Rule.

Certain responsibilities of the Security Officer may be delegated to a designee. If a different Clay County department or role is responsible for a certain responsibility, it shall be noted in this Policy.

ADMINISTRATIVE, PHYSICAL, & TECHNICAL SAFEGUARDS FOR ePHI

I. ADMINISTRATIVE SAFEGUARDS[2]

The Security Officer, in conjunction with the Privacy Officer, is responsible for creating, implementing, and maintaining the following administrative safeguards below to ensure the confidentiality and availability of ePHI held by the Clay County.

A. Security Management Program[3]

The Security Officer is responsible for adopting and implementing a program to comply with the HIPAA Security Rule. The Security Management Program includes: (a) a Risk

[2] HIPAA Security Rule § 164.308
[3] HIPAA Security Rule § 164.308 (a)(1)

Analysis, (b) a Risk Management Plan, (c) a Sanctions/Disciplinary Policy, and (d) a System Activity Review.

1. Risk Analysis

The Risk Analysis determines the overall level of risk to ePHI held by the Clay County. The Security Officer is responsible for conducting this Risk Analysis[4]. When conducting the Risk Analysis, the Security Officer shall (a) identify assets and Systems that create, receive, transmit, or maintain ePHI and (b) complete a technical and non-technical assessment to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. These technical and non-technical assessments must be completed on an annual basis[5] or whenever there is a material change in business practices that may affect the security or integrity of PHI.

(i) Technical Assessment.

The Security Officer shall perform a technical assessment on Clay County Systems to check the adequacy of System controls within its network architecture, operating system environments, and applications. The Security Officer shall also perform technical tests on the System to determine the correctness and functionality of the security controls, which may include vulnerability scans and penetration tests.

(ii) Non-Technical Assessment.

The Security Officer shall perform reviews and analyses to assess compliance with non-technical security controls ("Non-Technical Assessment"). Non-Technical Assessments could include: (1) using social engineering techniques to assess Workforce Member's retention of and compliance with security awareness training; (2) reviewing this Policy and associated policies, procedures, and documentation for maintenance, correctness, and completeness; and (3) reviewing System network architecture for maintenance, correctness, and completeness.

2. Risk Management Plan

Using the results from the Risk Analysis, the Security Officer, along with the Privacy Officer and Risk Manager, is responsible for creating and implementing the "Risk Management Plan", which shall include policies and procedures identified by the Security Officer to reduce risks and vulnerabilities of the System to a reasonable and appropriate level, based on the Clay County's risk appetite and risk tolerance.

[4] The risk analysis performed shall use the Security Risk Assessment (SRA) developed by the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR).
[5] Minnesota Statutes, Minn. Stat. § 13.055(6).

3. Sanctions/Disciplinary Policy

The Security Officer, in collaboration with the Clay County's legal department and/or human resources team, is responsible for applying sanctions and/or discipline in the event of a suspected violation of this Policy. Please see the HIPAA Sanctions / Disciplinary Policy as set forth in these HIPAA Privacy and Security Policies and Procedures for more information.

4. System Activity Review

The Security Officer is responsible for implementing policies and procedures to regularly review System activity, such as audit logs, access reports, and Security Incident tracking reports. The Security Officer shall:

(a) Monitor and review activity logs, active user accounts and Devices on a periodic basis as determined by the Security Officer;

(b) Lock user accounts when deemed necessary by the Security Officer;

(c) Utilize tools and process to monitor activity logs;

(d) Obtain basic user access reports, as needed; and

(e) Manually track security incidents, as needed.

B. Workforce Member Security[6]

The Security Officer, in coordination with Program Leaders, are responsible for implementing security policies and procedures to ensure that only authorized Workforce Members have access to ePHI.

1. Authorization and Supervision

The applicable Program Leader will determine those Workforce Member groups who are authorized to access ePHI. The applicable Program Leader shall determine the categories of ePHI that department Workforce Members are authorized to access. Each Workforce Member will be assigned appropriate security oversight, training, and access based on the ePHI access required for the Workforce Member to complete their essential job functions.

2. Workforce Member Clearance Procedure

The applicable Program Leader shall ensure that appropriate employment screening measures are employed on Workforce Members who will have access to ePHI. Before establishing access for Workforce Members who are authorized to access PHI, the applicable Program Leader will ensure that such Workforce Member executes a

[6] HIPAA Security Rule § 164.308 (a)(3)

confidentiality agreement containing obligations of confidentiality and nondisclosure with respect to the Processing of ePHI (See Appendix II – Form 1).

3. Termination Procedures

Upon termination of employment of any Workforce Member authorized to access ePHI, the applicable Program Leader shall notify the Security Officer of the Workforce Member's last working day. The Security Officer shall immediately terminate the Workforce Member's System access after that date. Items used to gain physical access to Clay County facilities (e.g., keys, IDs, access codes, badges, etc.) shall be relinquished and provided to the applicable Program Leader.

C. Information Access Management[7]

1. Access Authorization

The applicable Program Leader will inform the Security Officer of the necessary System access permissions for each Workforce Member. The Security Officer will set the permissions as instructed.

2. Access Establishment and Modification

Workforce Member access profiles will be reviewed and audited by applicable Program Leaders and IT Workforce Members periodically and as requested by such applicable Program Leaders. Program Leaders shall notify the Security Officer if a Workforce Member's access privileges need to be revised.

D. Security Awareness and Training[8]

The Security Officer, in coordination with applicable Program Leaders, are responsible for developing and delivering a security awareness and training program and periodically reviewing and updating training material based on the evolving needs of the Clay County. Security training will be delivered to all Workforce Members as a part of their onboarding process with the Clay County and periodically thereafter on an as needed basis. Education and training on security awareness may include, at a minimum, the following topics: (1) information access control, (2) incident reporting, (3) viruses and malicious software vigilance and reporting, (4) user log in monitoring and reporting, (5) password maintenance hygiene, (6) social engineering training, and (7) general training on the handling of ePHI, and (8) annual required training on data privacy, data security, and protecting information by the Minnesota Department of Human Services.

[7] HIPAA Security Rule § 164.308 (a)(4)
[8] HIPAA Security Rule § 164.308 (a)(5)

1. Protections Against Malicious Software

The Security Officer shall ensure the following security measures are implemented to protect again malicious software:

(a) Maintenance of up-to-date firewalls and installation of tested and approved security patches as soon as is reasonably practicable;

(b) Installation of anti-virus protection and spyware detection software on all computers and other associated electronic Devices that are connected to any of Clay County's networked Systems; and

(c) Removal of any virus-infected computers or other electronic Devices from Clay County's network until such Devices are verified as virus-free.

The Security Officer shall make all Workforce Members aware of the following rules with respect to encountering and preventing malicious access to Systems described below as well as the additional rules laid out in Clay County's Acceptable Use Policy.

(a) Workforce Members shall not disable any protections installed by IT against malicious software.

(b) Workforce Members shall act vigilant against any suspicious electronic communications and shall not open any e-mail attachments or links that are received from an unknown source or that are considered suspicious.

(c) Workforce Members shall not download any software from the Internet, or install any software, without prior approval of the Security Officer.

(d) Workforce Members shall not copy any information from a portable storage medium to a Clay County computer unless the storage medium has been approved by IT.

(e) Workforce Members shall immediately report to the Security Officer any suspicions of malicious activity on the System, or any malicious software downloaded to any electronic Device connected to the System.

2. Log-In Monitoring

The Security Officer will be responsible for implementing log-in monitoring and recording mechanisms on Clay County's System. Such mechanisms will include, for example, locking out a user from Clay County's network after a number of unsuccessful attempts within a certain time period of minutes, as periodically determined by the Security Officer.

3. Password Management

The Security Officer shall make all Workforce Members aware of the following rules with respect to password management, and all Workforce Members shall ensure that he or she complies with the following rules described below.

(a) Workforce Member user passwords should be complex based on IT department standards and shall be changed periodically within timeframes determined by the Security Officer or when there is reason to believe that the password has been compromised.

(b) Workforce Member user IDs and/or passwords should not be written down and kept within the general area of the computer or stored on-line.

E. Contingency Plan[9]

The Security Officer shall create processes and procedures needed to (a) recover access to ePHI and (b) ensure continuation of critical business functions during the emergency event ("Disaster Recovery Plan").

The Disaster Recovery Plan shall include:

(a) A data back-up plan, which establishes and implements procedures to create and maintain retrievable exact copies of ePHI;

(b) Disaster recovery procedures to restore any loss of data; and

(c) An emergency mode operation plan, establishing procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

The Security Officer shall also be tasked with regularly evaluating the effectiveness of the Clay County's Disaster Recovery Plan and updating or revising as necessary to ensure the protection and timely resumption of essential operations.

Further, the Security Officer shall perform periodic technical and nontechnical evaluations based upon this Policy and in response to environmental or operational changes affecting the security of ePHI to establish the extent to which the Clay County's or a Business Associate's security policies and procedures meet the requirements of HIPAA Security Rule.[10]

[9] HIPAA Security Rule § 164.308 (a)(7)
[10] HIPAA Security Rule § 164.308 (a)(8)

On a periodic basis, the Security Officer shall:

(a) Perform monitoring of the health/performance of Systems;

(b) Maintain hardware to ensure availability;

(c) Implement redundancy and failover as appropriate or feasible for all critical Systems;

(d) Provide adequate communications bandwidth and redundancy;

(e) Keep current with all vendor-recommended System upgrades and software patches and patches for known vulnerabilities;

(f) Guard against malicious actions;

(g) Evaluate server rooms and IDF closets for their criticality to the offices they serve and ensure all rooms storing sensitive data will be identified;

(h) Implement appropriate environmental controls for access, cooling, backup power and fire suppression for all server rooms and IDF closets and ensure that alerts are provided in the event of failure;

(i) Ensure that all equipment is stored in a locked environment, as appropriate;

(j) Protect Systems against environmental hazards;

(k) Maintain appropriate backup controls; and

(l) Develop recovery time objectives and recovery point objectives for Systems.

II. PHYSICAL SAFEGUARDS[11]

The Security Officer is responsible for implementing and monitoring the following physical safeguards below to prevent unauthorized physical access to ePHI, while ensuring continued access to such Systems for authorized Workforce Members.

A. Facility Access Controls[12]

The Security Officer shall identify potential physical security vulnerabilities in the facilities and based on such identified vulnerabilities, propose and implement corrective measures. The Security Officer shall also implement policies and procedures to limit physical access to any facility where Clay County Systems are housed.

[11] HIPAA Security Rule § 164.310
[12] HIPAA Security Rule § 164.310 (a)

1. Contingency Operations

The Security Officer shall create, implement, and monitor procedures that will permit authorized Workforce Members access to the Clay County's facilities to restore lost ePHI during an emergency in accordance with the Disaster Recovery Plan.

2. Facility Security

The Security Officer shall implement procedures to prevent the unauthorized physical access, tampering, and/or theft of the Clay County's facilities/equipment, such as through the use of access key cards and readers, secured desks, and locked cabinets.

3. Access Control and Validation

The Security Officer shall implement and monitor procedures to (a) validate access to the Clay County's facilities based on a Workforce Member's role within the organization or a visitor's reason for accessing the facility and (b) control access to Systems for revision or testing purposes. Access key card attempts are logged with a date and time stamp and access logs are reviewed on a periodic and as needed basis. Particularly, the Privacy Officer reviews access logs for areas that contain federal tax information on a monthly basis and all other access logs on a quarterly basis.

4. Facility Maintenance

The Security Officer and the Facility's Director shall implement and monitor procedures to ensure the proper (a) maintenance of all security features of the Clay County's facilities and (b) documentation of any installation, repairs, or changes to security features of Clay County's facilities (e.g., hardware, walls, doors, and locks). Such documentation shall be maintained by, as appropriate, the Security Officer.

B. Device Use[13]

The Security Officer shall maintain an inventory of all Clay County-owned Devices. The Security Officer and/or Program Leader shall implement policies and procedures to cover each Device type that describe:

(a) The proper functions that may be performed on Devices containing ePHI;

(b) The manner in which those functions may be performed; and

(c) The appropriate physical surroundings needed for Devices that access ePHI.

[13] HIPAA Security Rule § 164.310 (b)

C. Device Security[14]

The Security Officer shall implement and monitor appropriate physical measures to limit unauthorized access to ePHI on Devices. Such physical measures shall include:

(a) Incorporating security controls on Devices including passwords, hard drive encryption, and multi-factor authentication; and

(b) Implementing security measures that would require a unique User ID and password for any remote access to Clay County's network.

The Program Leader shall make all Workforce Members aware of policies and procedures with respect to Device security. Each Workforce Member shall ensure that he or she complies with the following rules described below.

(a) Workforce Members shall not: (i) disclose his/her password or log in details or (ii) share or loan to anyone a key, proximity card, or any other physical device permitting access to facilities where ePHI is stored.

(b) Workforce Members shall immediately report lost or stolen Devices or suspicious attempts to gain access to Devices or other equipment containing ePHI to their Program Leader, who shall notify the Clay County Security Officer.

(c) Workforce Members who have been approved to work remotely shall: (i) access ePHI on only approved Clay County-owned Devices and only through an Clay County approved encrypted connections (i.e., no public Wi-Fi) and multi-factor authentication measures, (ii) terminate remote access when no longer in active use, and (iii) not download or copy ePHI from any Device to any non-Clay County provided equipment, including personally owned equipment, (*e.g.*, thumb drive, tablet, CD), without the prior authorization of the Security Officer.

(d) Once VPN connection is made, all traffic must go through that connection and a separate connection must be restricted.

D. Device and Media Controls[15]

The Security Officer shall implement procedures regarding the receipt, re-use, disposal, and movement of Devices containing ePHI into, out of, and within Clay County facilities.

Such policies and procedures include: (a) a process that records the destruction, re-use, and movements of Devices and Electronic Media and (b) a data backup and storage process to ensure a copy of ePHI is maintained by the Clay County prior to the destruction, re-use, or movement of any Device or other removable Electronic Media.

[14] HIPAA Security Rule § 164.310 (c)
[15] HIPAA Security Rule § 164.310 (d)

The Security Officer shall:

(a) Reallocate the Device only after (i) such Device is properly returned, accounted for, and updated in the master inventory list and (ii) prepared for proper re-use by the Security Officer (such as securely overwriting components on which sensitive data is stored);

(b) Store backups in a secure location and in a manner that it is only accessible by authorized Workforce Members;

(c) Complete requests for data restoration from backup media only after the requester's identity has been verified; and

(d) Destroy and move Devices or Electronic Media in the manner as specified below.

1. Destroying Devices & Other Electronic Media Containing ePHI

The Security Officer shall implement and maintain policies and procedures governing the destruction of Device hardware and other Electronic Media containing ePHI which require that the Security Officer:

(a) Destroy Devices and Electronic Media in a manner that renders the ePHI unrecoverable;

(b) Wipe clean the memories of all printers, scanners, copy machines, and electronic fax machines before decommissioning, returning, selling, recycling, destroying, or sending such equipment outside of the Clay County's facilities for repair;

(c) Dispose of any backup media containing ePHI when no longer needed, in a manner that renders the ePHI unrecoverable; and

(d) Update the master inventory list, thereby showing that such Device hardware and/or Electronic Media has been destroyed.

2. Moving Devices & Other Electronic Media Containing ePHI

The Security Officer shall be responsible for tracking and recording the movement of Devices and IT-approved removable Electronic Media containing ePHI within Clay County. When necessary, applicable Program Leaders shall request from the Security Officer a backup copy of any ePHI prior to moving the Device.

E. Special Rules Regarding The Treatment Of Phi Held In Paper Files

Program Leaders shall make all Workforce Members aware of policies and procedures with respect to the proper Processing of PHI contained in paper files. Each Workforce Member shall ensure that he or she complies with the following rules described below.

(a) Workforce Members with a need to remove PHI from Clay County facilities for the performance of job duties and legitimate business reasons may do so if the PHI is secured in a locked container or briefcase.

(b) Paper records are not to remain off-site for a longer period than needed to perform job duties.

(c) Workforce Members authorized to take paper records containing PHI off-premises are responsible for ensuring the security of such records while they are off-site.

(d) Paper documents and files containing PHI will be maintained in a restricted area that can be accessed only upon showing proper identification. Paper documents and files containing PHI, when unattended, shall be maintained in a secure area, such as a locked file drawer, locked file cabinet, or locked office. Only Workforce Members authorized to access the applicable PHI will have access to the key(s) to the secure area where PHI is left unattended.

(e) All originals, copies, and scans of documents containing PHI will be removed from the copier or scanner immediately upon completion of the copy job or the scan. Copying or scanning of such documents should be kept to the minimum necessary; only the number of copies needed should be made. Any unwanted copies should be shredded before being discarded.

(f) When Workforce Members print any document containing PHI to a printer in a public area, they will immediately retrieve the document from the printer. Workforce Members should print electronic documents containing PHI only to the minimum extent necessary to accomplish a legitimate business purpose.

(g) When documents containing PHI have met their retention requirements, only Workforce Members authorized to access PHI will move paper files containing PHI from the secure area in which the files are normally stored to a storage box. The storage box will be maintained securely until destroyed. Only Workforce Members authorized to access the applicable PHI will have access to the key(s) to the secure area where the boxed PHI is stored.

(h) When a paper file containing PHI needs to be destroyed, the file will be shredded and stored in secured locked bins.

III. TECHNICAL SAFEGUARDS[16]

The Security Officer shall be responsible for implementing and monitoring policies and procedures governing technical access controls with respect to Devices or Systems Processing ePHI. Such policies and procedures include rules governing (a) the use of

[16] HIPAA Security Rule § 164.312

unique user ID and passwords, (b) audit controls, (c) rules to protect the integrity of ePHI, and (d) security controls when ePHI is transmitted into and out of Clay County Systems.

A. Access Control[17]

1. Unique User Identification

The Security Officer shall ensure that all Workforce Members have been assigned a unique user ID when accessing Clay County Systems and/or Devices. Such user IDs will be monitored by the Security Officer for inactivity.

2. Emergency Access Procedure

The Security Officer shall create, implement, and monitor procedures to ensure access to ePHI in the event of an emergency.

3. Automatic Logoff

The Security Officer shall ensure that all Devices have appropriate measures installed to lock the Device during periods of inactivity to prevent unauthorized or casual viewing of ePHI.

4. Encryption and Decryption / Data protection

The Security Officer shall make all Workforce Members aware of policies and procedures with respect to data encryption or protection. EPHI at rest shall be encrypted as necessary.

Each Workforce Member shall ensure that he or she only transmits ePHI in using an approved encryption measures approved by the IT Department.

The following restrictions shall apply to the storage of ePHI:

(a) ePHI stored in emails/Outlook shall be saved in approved Clay County Systems and then deleted;

(b) No ePHI may be included on calendar entries;

(c) No ePHI may be included in third party chats communications or other third-party meeting platforms;

(d) Mobile Devices and portable storage medium that store ePHI must be encrypted; and

(e) Devices may not be in the vicinity of cameras and cameras may not be used to take photos which include Device screens.

[17] HIPAA Security Rule § 164.312 (a)

B. Audit Controls[18]

The Security Officer will be responsible for regularly examining, monitoring, and recording System activity by automated and/or human means for data loss prevention and for unauthorized Processing of ePHI, which shall include reviewing summaries and analyses of System and/or Device audit trails and activity logs during regular Systems Activity Reviews or in the event of suspected violations of this Policy.

The Security Officer will ensure that appropriate Systems and/or Devices containing ePHI incorporate basic audit trails that record the Workforce Member Processing of ePHI in such Systems and/or Devices. To the extent feasible, the following information may be recorded in the audit trails:

(a) Successful and/or rejected System and/or file access;

(b) Device identification and/or location;

(c) User identification;

(d) File creation, modification, and/or deletion (including who performed such activity); and

(e) System configuration setting modifications.

C. Integrity – Mechanism to Authenticate ePHI[19]

Program Leaders shall be responsible for creating, implementing, and monitoring mechanisms and procedures to (a) authenticate ePHI and (b) corroborate that ePHI has not been altered or destroyed. When creating data integrity and loss prevention procedures, Program Leaders shall identify (a) all approved users with the ability to alter or destroy ePHI, (b) the scenarios that may result in the unauthorized modification to or destruction of ePHI, and (c) the potential individuals or groups who may engage in such unauthorized modification to or destruction of ePHI.

D. Person/Entity Authentication[20]

The Security Officer shall be responsible for creating, implementing, and monitoring mechanisms and procedures to authenticate an individual's identity when seeking access to ePHI.

[18] HIPAA Security Rule § 164.312 (b)
[19] HIPAA Security Rule § 164.312 (c)
[20] HIPAA Security Rule § 164.312 (d)

E. Transmission Security[21]

The Security Officer shall implement and maintain the technical security measures to protect ePHI from improper alteration or destruction and to guard against unauthorized access to ePHI while in transit from Clay County-approved Systems to external electronic communications networks. Such measures shall include: (i) integrity controls and (ii) encryption measures.

1. Integrity Controls

The Security Officer shall implement and maintain security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

2. Transmission Encryption and Protection

The Security Officer will be responsible for implementing mechanisms with respect to the encryption of ePHI while transmitted over the Internet.
The Program Leader shall make all Workforce Members aware of policies and procedures with respect to the transmission of ePHI outside of the System.

F. General Rules for All Electronic Transmissions of ePHI

To safeguard ePHI, all Workforce Members, when receiving or transmitting ePHI, shall complies with the following rules described below.

Workforce Members shall:

(a) Authenticate the proposed receiving person or entity and ensure that any emails containing ePHI has a confidentiality statement that provides specific directions on the steps to take if the electronic transmission is sent to the wrong location / person, including any directions to return or delete the misdirected email;

(b) Include only the minimum ePHI needed to complete the purpose of the transmission;

(c) Adhere to integrity controls instituted by the Security Officer when storing or transmitting ePHI over any communications network (including wireless networks);

(d) Ensure that all e-mail communications containing ePHI are encrypted using the Clay County's industry standard or better encryption platforms;

[21] HIPAA Security Rule § 164.312 (e)

(e) Contact the sending party directly over the phone if Workforce Members must confirm receipt of ePHI;

(f) When approved to work remotely, ensure Devices used to send and receive emails containing ePHI are secure and in work areas that ensure confidentiality;

(g) Upon receipt of an e-mail with an attachment containing ePHI, save the attachment to a drive that has full disk encryption for Systems; and

(h) Download and save any emails with attachments containing ePHI to authorized locations on the System and may never store ePHI on a local hard drive of a Device, or portable storage medium (*e.g.*, laptop, CD, thumb drive, etc.), except as expressly authorized by the Security Officer.

G. Rules Regarding Fax Transmission of ePHI

All Workforce Members who send or receive ePHI via electronic fax shall adhere to the following requirement: Workforce Members shall ensure that each facsimile containing PHI must be accompanied by a cover sheet containing a clear and legible confidentiality notice. The confidentiality statement on the fax cover sheet and/or the electronic transmission shall provide specific directions on the steps to take if the fax is sent to the wrong location / person. The cover sheet will either ask the recipient to return or destroy the misdirected fax.

A sample statement is as follows:

This facsimile transmission and any documents accompanying this fax contain confidential information belonging to the sender. This information may be legally privileged. This information is only for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking of any action in reliance on or regarding the contents of this facsimile is strictly prohibited. Any individual receiving this transmission, who is not the intended recipient, is requested to notify the sender by return fax or by the telephone number listed on the fax. If there is no contact number, the item(s) must be destroyed.

DISCLOSURES OF ePHI TO BUSINESS ASSOCIATES & OTHER THIRD PARTIES

The Clay County will permit a Business Associate to Process ePHI on its behalf only if the Business Associate has (a) undergone appropriate due diligence on its security and business continuity measures and (b) contractually agreed to appropriately safeguard the ePHI in accordance with the requirements under the HIPAA and containing acceptably similar protections of ePHI found in Clay County's "Business Associate Agreement Template" (See Attachment II, Form 15).

Workforce Members shall obtain the authorization of the Security Officer prior to granting a Business Associate access to any System containing ePHI. If System access is approved by the Security Officer, the Business Associate will be issued log-in credentials, either on an

individual or Business Associate-wide basis, for a temporary time period. These credentials shall be de-activated when not needed and deleted when the relationship is terminated.

SECURITY INCIDENT RESPONSE

Please see the Incident Response and Breach Notification section of the Policy below for further information.

POLICY MAINTENANCE, CHANGES, & DOCUMENTATION

The Security Officer and Privacy Officer will ensure the periodic review of this Policy in response to environmental, legal, or operational changes affecting the security of PHI and will update the Policy and any associated policies and/or procedures, to the extent necessary. The Privacy Officer shall ensure that any changes made to this Policy, and all documentation related to it are properly documented in writing and maintained in the Clay County's records for at six (6) years or for longer periods of time as required under applicable state law. The Privacy Officer shall ensure that all documentation is available to those Workforce Members responsible for these procedures.

The Privacy Officer will ensure that all Workforce Members are made aware of any changes to this Policy and any associated policies and/or procedures. For the avoidance of doubt, the Clay County reserves the right to amend or change this Policy at any time without notice, and all Workforce Members shall be responsible for complying with the most recent version of this Policy.

INCIDENT RESPONSE AND BREACH NOTIFICATION

Policy

Clay County and its Business Associates will strive to maintain privacy and security measures intended to protect the confidentiality and integrity of PHI. Pursuant to HIPAA, Clay County will notify individuals when there is a Breach of Unsecured PHI that does not fall within a statutory exception or when there is more than a low probability that the PHI has been compromised. When required under HIPAA and other data breach notification laws, Clay County will also notify OCR and/or other governmental or external third parties, as applicable.

Specific incident response procedures under the Clay County Incident Response Plan shall be adhered to and incorporated into this section.

Obligations of the Privacy Officer and Security Officer that are referenced throughout this section may be designated to other roles and/or teams as described in the Clay County Incident Response Plan such as the Chief Information Officer, the Incident Response Commander, the Cyber Security Incident Handling Team, the Cyber Security Incident Response Team, the Recorder, and other Incident Response Team Members.

Procedure

Discovery, Communication, and Investigation of an Incident.

In the event a suspected incident involving the potential unauthorized use or disclosure of PHI, which may or may not be a Security Incident ("Incident"), is discovered by a Workforce Member, the following steps shall be taken:

1. The Workforce Member who discovered the Incident shall immediately notify the Privacy Officer once he or she learns of the Incident through the submission of an Incident Report Form (see Appendix II, Form 14).

2. If the Incident involved a potential IT vulnerability or a breach of security measures, the Privacy Officer shall immediately notify the Security Officer to contain the Incident and mitigate any potential harm as a result of the Incident.

3. The Privacy Officer shall gather facts and investigate the nature of the Incident. The reporting Workforce Member shall fully cooperate with the Privacy Officer's investigation.

4. Once the investigation is complete, the Privacy Officer shall develop an action plan to address the Incident, which shall be reviewed by senior Clay County management, and, to the extent necessary, legal counsel.

5. Throughout the investigation and response process, the Privacy Officer shall periodically keep Clay County senior management apprised of Incident response efforts.

6. The Privacy Officer shall provide information to relevant Program Leaders and Human Resources to address policy or program violations through disciplinary action, when necessary. PHI shall not be disclosed in this process.

7. In the event Clay County receives notification of an Incident from a Business Associate, the Privacy Officer or her/his designee shall coordinate with the Business Associate to ensure that all necessary information regarding the Incident and affected individuals is obtained in order for the above steps to be taken.

Determination of a Reportable Breach

After gathering facts and investigating the circumstances of the Incident, the Privacy Officer shall determine if the Incident is considered a Breach of Unsecured PHI that is reportable under HIPAA ("Reportable Breach"). This determination shall include the following steps:

1. Step 1 – Breach. Determine whether the Incident is considered a "Breach" under HIPAA. If the Incident is considered a Breach, the Privacy Officer or her/his designee will proceed to Step 2. If the Incident is not considered a Breach, no notification is required under this Policy.

2. Step 2 – Unsecured PHI. Determine whether the Incident involved "Unsecured PHI". If the Incident involved Unsecured PHI, the Privacy Officer or her/his designee will proceed to Step 3. If the Incident did not involve Unsecured PHI, no notification is required under this Policy.

3. Step 3 – Exclusions. Determine whether the Incident is excluded from the definition of the term "Breach." The three exclusions are as follows:

    (a) The unintentional acquisition, access, or use of PHI by a Workforce Member acting under the authority of a Covered Entity or Business Associate;

    (b) Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA; or

    (c) A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

If an exclusion applies, then no notification is required under the Policy. If an exclusion does not apply, then the Privacy Officer or her/his designee will proceed to Step 4.

4. Step 4 – Risk Assessment. Conduct a risk assessment to determine whether the Incident poses a significant risk of financial, reputational, or other harm to the affected individual(s), considering the following factors:

   (a) Who impermissibly used Unsecured PHI or to whom Unsecured PHI was impermissibly disclosed;

   (b) Whether the immediate mitigation actions taken by Clay County in response to the Incident eliminated or significantly reduced the risk of harm to the affected individual(s);

   (c) Whether Unsecured PHI was returned to Clay County without being accessed;

   (d) The nature, type and amount of Unsecured PHI that was improperly used or disclosed in connection with the Incident; and

   (e) Any other relevant factors regarding the Incident.

Procedure when Incident is NOT a Reportable Breach. If based on Steps 1-4 above, the Privacy Officer determines that the Incident not a Reportable Breach, the Privacy Officer shall document such conclusion and the rationale for such conclusion. Clay County shall maintain such documentation and any additional supporting documents for a period of at least six (6) years from the determination.

Procedure when Incident is a Reportable Breach. If based on Steps 1-4 above, Clay County determines that a Reportable Breach occurred, Clay County shall provide notice of the Reportable Breach in accordance with the "Providing Notice of a Reportable Breach" section below.

Providing Notice of a Reportable Breach

Notice to Affected Individuals.

Unless contrary instructions from law enforcement are received (see the "Procedure in the Event of a Law Enforcement Delay" *section below*), written notice of the Reportable Breach shall be provided to each affected individual, or each individual that is reasonably believed to have been affected by the Reportable Breach in the manner as described below.

1. *Timing of Notice.* The notice shall be provided promptly and no later than sixty (60) days after Clay County discovers the Reportable Breach. The Reportable Breach is considered to be discovered on the first day on which the Reportable Breach is known, or should have been known by exercising reasonable diligence to any person who is a Workforce Member or Business Associate of Clay County (other than the person committing the Reportable Breach).

2. *Manner of Notice*. The notice shall be sent by first-class mail addressed to the last known address of the individual. Notice may be sent electronically if the individual has agreed to receive electronic notice and the agreement has not been withdrawn. If Clay County knows that the individual is deceased, Clay County shall provide written notice to the next-of-kin or personal representative of such person if Clay County has the address of that individual. Notice may be provided in one or more mailings as additional information becomes available.

3. *Content of Notice*. The notice shall be written in plain language and shall contain the following information:

   (a) A brief description of the Reportable Breach, including the date of the Reportable Breach and the date of the discovery of the Reportable Breach if known;

   (b) A description of the types of Unsecured PHI involved in the Reportable Breach (rather than a description of the specific PHI);

   (c) Any steps the individual should take to protect himself or herself from harm resulting from the Reportable Breach;

   (d) A brief description of what Clay County is doing to investigate the Reportable Breach, to mitigate the harm to the individual and to protect against future occurrences; and

   (e) Contact procedures for the individual to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

4. *Substitute Notice.* If there is insufficient or out-of-date contact information for an individual that precludes written notice to such person, as soon as reasonably possible after such determination, Clay County shall provide notice reasonably calculated to reach the individual as described below.

   (a) If there is insufficient or out-of-date contact information for fewer than ten (10) individuals, notice may be provided by e-mail, telephone, or other means.
   (b) If there is insufficient or out-of-date contact information for ten (10) or more individuals, notice shall:

(i) Be in the form of either a conspicuous posting for ninety (90) days on Clay County's website home page or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and

(ii) Include a toll-free number that remains active for at least ninety (90) days so that the individual can learn whether his or her Unsecured PHI was included in the Reportable Breach.

(c) Substitute notice need not be provided if the affected individual is deceased, and Clay County has insufficient or out-of-date contact information for the next-of-kin or personal representative of the individual.

5. *Additional Notice in Urgent Situations*. If Clay County determines there is potential for imminent misuse of the Unsecured PHI in connection with a Reportable Breach, Clay County may provide information regarding the Reportable Breach to individuals by telephone or other means, as appropriate, in addition to providing the required written notice as described above.

Notice to HHS

Unless contrary instructions from law enforcement are received (see the "Procedure in the Event of a Law Enforcement Delay" *section below*), in addition to notifying individuals as described above, Clay County also shall notify OCR of a Reportable Breach. Such notification shall be provided as follows:

1. *If the Reportable Breach involves 500 or more individuals*: Clay County shall notify HHS of the Reportable Breach contemporaneously with providing notice to individuals and in a manner specified by HHS on its website.

2. *If the Reportable Breach involves less than 500 individuals*: Clay County shall maintain a log or similar documentation of the Reportable Breach and shall provide the required documentation to HHS no later than sixty (60) days after the end of each calendar year in which a Reportable Breach occurred in the manner specified by HHS on its website.

Notice to the Media

Unless contrary instructions from law enforcement are received (see the "Procedure in the Event of a Law Enforcement Delay" *section below*), if a Reportable Breach involves more than 500 residents of a particular state or jurisdiction, in addition to notifying the individual and HHS, Clay County also shall notify prominent media outlets serving the state or jurisdiction. Such notice shall be provided promptly and in no case later than sixty (60) calendar days after discovery of the Reportable Breach. The notice shall contain the same information included in the notice to the individual.

Procedure in the Event of a Law Enforcement Delay.

If a law enforcement official informs Clay County that the notice to individuals, HHS or the media described above would impede a criminal investigation or cause damage to national security, Clay County shall comply with the delay as described below.

1. *If the statement is in writing and specifies the time for which a delay is required*: delay the notification for the specified time.

2. *If the statement is made orally*: document the statement, including the identity of the official, and delay the notification for no longer than thirty (30) days from the date of the oral statement, unless during that thirty (30) day period, the official provides a written statement requiring a different notification timeframe.

Notification Under Other Laws

The Privacy Officer shall also consider if an Incident requires notification to affected individuals, regulatory authorities, and/or other third parties under other applicable federal and state privacy, cybersecurity, and/or data breach notification laws, which may include notification and reporting requirements under the Minnesota Government Data Practices Act (Minnesota Statutes, Minn. Stat. § 13.055). In the event that notification is required, the Privacy Officer shall follow the notice requirements laid out under the applicable law.

Individual Complaint

Individuals affected by the Reportable Breach have the right to complain to Clay County and/or OCR if they believe their privacy rights have been violated. In the event of an individual complaint, the "Individual Rights – Right to File a Privacy Complaint" section of this Policy should be followed.

Post Incident Review and Actions

If deemed necessary, the Security Officer shall conduct a post-incident review of any deficiencies in data security measures and/or internal policies or procedures that may have contributed to the Incident and adjust these measures and/or policies as needed to prevent similar Incidents from occurring in the future. If deemed necessary, the Privacy Officer and/or Security Officer may require applicable Workforce Members to complete refresher security and/or data protection training. The Privacy Officer may also apply disciplinary action to Workforce Members whose actions contributed to the Incident if disciplinary action is considered necessary based on the facts and circumstances surrounding the Incident.

Documentation

The Privacy Officer shall maintain a written record or log all Reportable Breaches regardless of the number of individuals affected. The Privacy Officer shall also maintain the documentation related to the provision of notice to individuals, HHS, the media, if applicable, and any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date notice was provided

To the extent an impermissible disclosure of unsecured PHI occurred, regardless of whether notification was required, a log of the disclosure may be required to be included in the accounting of disclosures as described in the "Individual Rights – Right to Accounting of Disclosures of PHI" section of this Policy.

Training

Clay County shall maintain a policy and train Workforce Members to alert the Privacy Officer immediately upon discovery or suspicion of improper use or disclosure of PHI.

ATTACHMENT:
APPENDIX II – Form 14 – Incident Report Form

BUSINESS ASSOCIATES

Prior to any PHI being shared with a Business Associate, there must be a written agreement between Clay County and the Business Associate under which the Business Associate must appropriately safeguard the PHI and comply with HIPAA and Clay County Privacy Policies. A Business Associate must comply with the HIPAA and Clay County's Privacy Policies to the same extent, and is subject to the same penalties, as Clay County. A Model Business Associate Agreement template is located in Appendix II, Form 15.

An agreement is not required if the Business Associate is a health care provider performing functions or providing services for purposes of treating an individual.

Elements of Agreement.

The agreement must contain the following provisions:

(i) A statement that the Business Associate must comply with all of the requirements imposed under HIPAA;

(ii) A description of how the Business Associate may use PHI disclosed to it, a requirement that the Business Associate use appropriate safeguards to prevent any other uses, and a requirement that the Business Associate mitigate any harmful effect known to it of a use or disclosure that violates the agreement;

(iii) A prohibition on any use or disclosure of PHI which violates HIPAA or this Policy;

(iv) A statement that the Business Associate, in using or disclosing PHI, complies with the minimum necessary policies and procedures of Clay County, which includes limiting the use or disclosure to a limited data set as defined in HIPAA, unless the Business Associate and/or Clay County determines that a limited data set is not practicable;

(v) A statement that the Business Associate must report to Clay County any use or disclosure of PHI not permitted under the agreement, and must also comply with the Breach Notification requirements for a breach of unsecured PHI (which is PHI that is not encrypted, or otherwise shredded or physically destroyed);

(vi) A requirement that any subcontractors of the Business Associate that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree in writing to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such information and sign a Business Associate agreement with the Business Associate to that effect;

(vii) To the extent the Business Associate is to carry out a Clay County obligation under Subpart E of 45 CFR Part 164, it shall comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(viii) A statement that the Business Associate must cooperate in honoring an individual's or a children's/guardian's rights to access PHI, to request amendments, and to receive an accounting of disclosures of PHI;

(ix) A requirement that the Business Associate make its records available for audit by the Secretary of Health and Human Services for monitoring compliance with HIPAA and this Policy, and shall also make its records available to Clay County;

(x) A statement that the Business Associate shall comply with the Security Rule within HIPAA, including ensuring the confidentiality, integrity, and availability of electronic PHI, implementing safeguards, ensuring that agents and subcontractors do the same, developing and enforcing appropriate policies and procedures, and reporting security incidents to Clay County;

(xi) A requirement that, on termination of the agreement, the Business Associate return or destroy all PHI (or if that is not feasible, continue to protect the confidentiality of PHI); and

(xii) A provision that allows Clay County to terminate the agreement if the Business Associate has violated a material term of the agreement (other than a required termination as further described below).

The agreement may also permit the Business Associate to use information it receives for the proper management of its business, to carry out its legal responsibilities, or for data aggregation purposes. The agreement may also include a statement that the Business Associate, and not Clay County, is liable for any breaches of PHI by the Business Associate's subcontractor.

Required Termination of Agreement.

If Clay County or the Business Associate comes to know of a pattern of activity or practice of the other party that violates its obligations under the agreement, and violating party does not halt or remedy this activity or practice, then Clay County or Business Associate must either terminate the agreement or report the problem to the Clay County General Privacy Officer.

ATTACHMENT:

APPENDIX II – Form 15 – Model Business Associate Agreement

EDUCATION, TRAINING, AND AWARENESS OF HIPAA

This Policy establishes a HIPAA training program for Clay County that includes a mandatory HIPAA training for all Workforce Members. Workforce Members who are volunteers, temporary employees, student interns, and contract employees shall receive basic HIPAA training. If deemed necessary by the Privacy Officer, additional skill-based training will be provided to those Workforce Members whose job duties are directly affected by HIPAA. Additional training requirements under the New Employee Orientation Policy shall be adhered to and shall be incorporated into this section.

1. Basic HIPAA Training. All Clay County Workforce Members must attend basic HIPAA training during new hire orientation and on an annual basis thereafter. If deemed necessary by the Privacy Officer, re-training sessions will be done on a periodic basis as needed. When the training is completed, the attendees should be able to:

    (a) Describe what HIPAA is and why it is in place today;
    (b) Know the current policies of the Clay County and how state law interacts with them;
    (c) Know what constitutes PHI;
    (d) Know the consequences for HIPAA violations;
    (e) Be aware of how HIPAA affects them in their workplace;
    (f) Know his/her obligation to report to the HIPAA Security Officer and HIPAA Privacy Officer any suspected incidents that involve impermissible use, access, acquisition, or disclosure of unsecured PHI, as soon as it is detected; and
    (g) Know whom to contact for additional assistance, as needed.

2. Specific HIPAA Training. Each Program Leader will identify and document the job categories within their departments that will need additional specific HIPAA training and the Privacy Officer, or designee, shall be responsible for administering the HIPAA training requirements specific to their own areas.

3. Documentation. All department training shall be documented and Workforce Members attending the training will be required to sign an attendance record, which shall be maintained for six (6) years. The attendance record will record the following:

    (a) Subject matter covered in the session;
    (b) Name of the presenter;
    (c) Date;
    (d) Time started and time ended;
    (e) Employee name; and
    (f) Employee job title/category.

SANCTIONS / DISCIPLINE FOR VIOLATIONS OF HIPAA

Policy

Clay County takes seriously the protection of PHI and its compliance with HIPAA. Therefore, it is the policy of Clay County to discipline Workforce Members who fail to comply with the Clay County's policies and procedures regarding HIPAA.

The Clay County reserves the right to take more serious disciplinary action than stated depending on the severity of the violation. This discipline could include any action up to and including termination of employment.

Please refer to discipline policy within Clay County's Personnel Policy for further rules regarding mandatory employee reporting of any known or suspected violations HIPAA.

Procedure

When a concern arises regarding a possible violation of the Policy or any HIPAA related procedure an investigation shall be commenced promptly.

If the conclusion of the investigation is that a violation of a HIPAA related procedure occurred, the Workforce Member may be disciplined in a manner that is appropriate to the nature and severity of the violation and based on the intent of the Workforce Member involved in the violation.

Applicable Workforce Members involved in the investigation shall document the facts surrounding the investigation, the outcome of the investigation, and, if applicable, the reason for the applying sanctions. Documentation from the investigation will be forwarded to the Privacy Officer to be maintained as a part of the Clay County's HIPAA documentation and retained for six (6) years.

Any disciplinary action documenting a Workforce Member's violation of the HIPAA policies or procedures will be coordinated with Human Resources and placed in the Workforce Member's personnel file. There will be no PHI shared or filed during this process.

APPENDIX I
STATE PRIVACY AND/OR CONFIDENTIALITY LAWS

Minnesota Health Records Act (MHRA), Minn. Stat. §144.291 - 144.298

Scope

The MHRA applies to “providers”. A “provider” means (i) any person who furnishes health care services and is regulated to furnish the services under the Minnesota statutes; (ii) a licensed home care provider; (iii) a licensed health care facility; (iv) a licensed assisted living facility; and (v) a registered physician assistant.[22]

The MHRA protects “health records” of “patients”. A "health record" means any information, whether oral or recorded in any form or medium, that (i) relates to the past, present, or future physical or mental health or condition of a patient; (ii) the provision of health care to a patient; or (iii) the past, present, or future payment for the provision of health care to a patient.[23]

A “patient” means (i) a natural person who has received health care services from a provider for treatment or examination of a medical, psychiatric, or mental condition, (ii) the surviving spouse and parents of a deceased patient, or (iii) a representative appointed in writing by the patient. In certain cases, patient can include a parent or guardian, or a person acting as a parent or guardian in the absence of a parent or guardian.[24]

Patient Rights

1. Privacy Notice.[25] A provider must provide a written notice to patients that include information on: (i) the types of disclosures of health records that may be made without the written consent of the patient, including the type of records and to whom the records may be disclosed and (ii) the patient’s rights to have access to and obtain copies of the patient's health records and other patient information maintained by the provider. The privacy notice may be provided with the copy of the patient bill of rights or displayed prominently in the provider’s place of business.

2. Access to Health Records.[26] Upon request, a provider shall supply to a patient within 30 calendar days of receiving a written request complete and current information possessed by the provider concerning any diagnosis, treatment, and prognosis of the patient. Unlike HIPAA, the MHRA does not have an access exception for psychotherapy notes and must be provided to the patient unless an exception under the MHRA applies (see below for further details). If requested, the provider must also provide (i) copies of the patient's health record, including but not limited to

[22] Minnesota Statutes, Minn. Stat. § 144.291.
[23] Minnesota Statutes, Minn. Stat. § 144.291.
[24] Minnesota Statutes, Minn. Stat. § 144.291.
[25] Minnesota Statutes, Minn. Stat. § 144.292.
[26] Minnesota Statutes, Minn. Stat. § 144.292.

laboratory reports, x-rays, prescriptions, and other technical information used in assessing the patient's health conditions or (ii) the pertinent portion of the record relating to a condition specified by the patient. With the patient's consent, the provider can provide only a summary of the health record. A provider may withhold information requested by the patient if the provider reasonably determines that the information is (i) detrimental to the physical or mental health of the patient or (ii) likely to cause the patient to inflict self-harm, or to harm another. The provider may supply the information to an appropriate third party or to another provider. The other provider or third party may release the information to the patient.

Rules on the Release / Disclosure of Health Records[27]

Under the MHRA, a person's health records cannot be released or disclosed without one of the following:

(i) A signed and dated consent from the patient or the patient's legally authorized representative authorizing the release;

(ii) A representation from a provider that holds a signed and dated consent from the patient authorizing the release; or

(iii) The disclosure is pursuant to a specific authorization under the law.

If a Covered Entity wishes to utilize a "specific authorization" under the law, the Covered Entity must document the release in the person's health record.

Specific Authorization Examples

1. Medical emergency.[28] Consent is not required during a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency.

2. Disclosure to related entities.[29] Consent is not required when disclosing health records to other providers within related health care entities when necessary for the current treatment of the patient.

3. Disclosure to a health care facility.[30] Consent is not required when disclosing health records to a licensed health care facility when a patient: (a) is returning to the health care facility and unable to provide consent; or (b) who resides in the health care facility, has services provided by an outside resource under Code of Federal Regulations, title 42, section 483.75(h), and is unable to provide consent.

4. Disclosure for purposes of diagnosing or treating a deceased person's surviving adult child.[31] A provider may release a deceased patient's health care records to

[27] Minnesota Statutes, Minn. Stat. § 144.293.
[28] Minnesota Statutes, Minn. Stat. § 144.293.
[29] Minnesota Statutes, Minn. Stat. § 144.293.
[30] Minnesota Statutes, Minn. Stat. § 144.293.
[31] Minnesota Statutes, Minn. Stat. § 144.293.

another provider for the purposes of diagnosing or treating the deceased patient's surviving adult child.

5. Disclosure to the Minnesota Commissioner of Health or the Health Data Institute.[32] Consent is not required for the disclosure of health records to the commissioner of health or the Health Data Institute under chapter 62J of the Minnesota Statutes, provided that the commissioner encrypts the patient identifier upon receipt of the data.

6. Disclosure to a record locator or patient information service.[33] A provider may release patient identifying information and information about the location of the patient's health records to a record locator or patient information service without consent from the patient unless the patient has elected to be excluded from the service. The Department of Health may not access the record locator or patient information service or receive data from the service. Only a provider may have access to patient identifying information in a record locator or patient information service. Except in the case of a medical emergency, a provider participating in a health information exchange using a record locator or patient information service does not have access to patient identifying information and information about the location of the patient's health records unless the patient specifically consents to the access. A provider must provide a mechanism for the patient to opt out of such sharing.

7. Emergency interaction with law enforcement (mental health crisis).[34] A health care provider must disclose health records relating to a patient's mental health to a law enforcement agency if (a) the law enforcement agency provides the name of the patient; (b) the law enforcement agency communicates that the patient is currently involved in a mental health crisis to which the law enforcement agency has responded; and (c) disclosure of the records is necessary to protect the health or safety of the patient or of another person. The scope of disclosure under this subdivision is limited to the minimum necessary for law enforcement to safely respond to the mental health crisis. The disclosure may include the name and telephone number of the psychiatrist, psychologist, therapist, mental health professional, practitioner, or case manager of the patient, if known; and strategies to address the mental health crisis. A law enforcement agency that obtains the health records shall maintain a record of the requestor, the provider of the information, and the patient's name. Health records obtained by a law enforcement agency under this scenario is considered "private data" on individuals as defined under the Minnesota Data Practices Act (see below for further details), and must not be used by law enforcement for any other purpose. A law enforcement agency that obtains health records under this situation shall inform the patient that health records were obtained.

[32] Minnesota Statutes, Minn. Stat. § 144.293.
[33] Minnesota Statutes, Minn. Stat. § 144.293.
[34] Minnesota Statutes, Minn. Stat. § 144.294.

8. Disclosure pursuant to independent medical examination.[35] A provider may release health records created as part of an independent medical examination to the third party who requested or paid for the examination.

9. Disclosures to juvenile court.[36] When any child shall be brought into juvenile court the court shall request, and the custodian of the record shall furnish, a complete certified copy of such record to the court, which copy shall be received as evidence in the case; and no decision or disposition of the pending matter shall be finally made until such record, if existing, shall be considered.

10. Disclosure for research purposes.[37] health records may be released to an external researcher solely for purposes of medical or scientific research subject to certain conditions.

11. Immunization Data.[38] Providers, schools, childcare facilities, community health boards, community action agencies and the Commissioner of Health may exchange immunization data with one another, without the patient's consent, if the person requesting access provides services on behalf of the patient. "Immunization data" means: (a) a patient's name, address, date of birth, gender, parent, or guardian's name and (b) the date the vaccine was received, vaccine type, lot number, and manufacturer of all immunizations received by the patient, and whether there is a contraindication or an adverse reaction indication.

12. Hepatitis B maternal carrier data; infant immunization.[39] The Commissioner of Health or a community health board may inform the physician, advanced practice registered nurse, or physician assistant attending a newborn of the hepatitis B infection status of the biological mother.

13. Permitted Disclosures under HIPAA. The Minnesota Supreme court ruled in 2023 that permitted disclosures under HIPAA qualify as "specific authorizations under law" under the MHRA.[40] Please see the "Permitted Uses and Disclosures of PHI" section of the Policy for further information on permitted disclosures under HIPAA.

Special Rules on Information Regarding Reproductive Health Care Services[41]

The MHRA makes clear that another state's subpoena or court order requiring the disclosure of reproductive health care services is not a "specific authorization" under the MHRA and would require patient consent. "Reproductive health care services" means medical, surgical, counseling, or referral services relating to the human reproductive

[35] Minnesota Statutes, Minn. Stat. § 144.297.
[36] Minnesota Statutes, Minn. Stat. § 144.30.
[37] Minnesota Statutes, Minn. Stat. § 144.295.
[38] Minnesota Statutes, Minn. Stat. § 144.3351.
[39] Minnesota Statutes, Minn. Stat. § 144.3352.
[40] *Schneider v. Children's Health Care*, 996 N.W.2d 197, 201 (Minn. 2023).
[41] Minnesota Statutes, Minn. Stat. § 144.2935.

system, including but not limited to services related to pregnancy, contraception, or the termination of a pregnancy.

Special Rules to Apply When Family Members Request Mental Health Information.

General Rule[42]

Upon the written request of a spouse, parent, child, or sibling of a patient being evaluated for or diagnosed with mental illness, a provider shall inquire of a patient whether the patient wishes to authorize a specific individual to receive information regarding the patient's current and proposed course of treatment. If the patient so authorizes, the provider shall communicate to the designated individual the patient's current and proposed course of treatment. If the spouse, parent, child, or sibling requests information about a patient who is being evaluated for or diagnosed with mental illness, the provider must notify the requesting individual of the right to have the provider request the patient's authorization to release information about the patient to a designated individual.

Exception[43]

A provider providing mental health care and treatment may disclose certain health record information (see below) about a patient to a family member or other person who requests the information if:

(a) The request for information is in writing;

(b) The family member or other person lives with, provides care for, or is directly involved in monitoring the treatment of the patient;

(c) The patient's mental health care provider, the patient's attending physician, or a person other than the person requesting the information has verified that the person requesting the information lives with, provides care for, or is directly involved in monitoring the treatment of the patient, and the request is documented in the patient's medical record;

(d) Before the disclosure, the patient is informed in writing of the request, the name of the person requesting the information, the reason for the request, and the specific information being requested;

(e) The patient agrees to the disclosure, does not object to the disclosure, or is unable to consent or object, and the patient's decision or inability to make a decision is documented in the patient's medical record; and

(f) The disclosure is necessary to assist in the provision of care or monitoring of the patient's treatment.

[42] Minnesota Statutes, Minn. Stat. §§ 144.294, 144.334.
[43] Minnesota Statutes, Minn. Stat. § 144.294.

The disclosed information must be limited to diagnosis, admission to or discharge from treatment, the name and dosage of the medications prescribed, side effects of the medication, consequences of failure of the patient to take the prescribed medication, and a summary of the discharge plan.

The provider must refuse to disclose the information if he/she/it reasonably determines that providing information would be detrimental to the physical or mental health of the patient or is likely to cause the patient to inflict self-harm or to harm another.

Special Rules on Copies of Video Tapes[44]

A provider may not release a copy of a videotape of a child victim or alleged victim of physical or sexual abuse without a court order or petition. This section does not limit the right of a patient to view the videotape.

Documentation[45]

Any release of health records without patient consent must be documented in the patient's health record. In the case of a release to a law enforcement agency, the documentation must include the date and circumstances under which the release was made, the person or agency to whom the release was made, and the records that were released.

When a health record is released using a representation from a provider that holds a consent from the patient, the releasing provider shall document: (i) the provider requesting the health records; (ii) the identity of the patient; (iii) the health records requested; and (iv) the date the health records were requested.

Health Care Bill Of Rights, Minn. Stat. § 144.651

Patients and residents shall, at admission, be told that there are legal rights for their protection during their stay at the facility or throughout their course of treatment and maintenance in the community and that these are described in an accompanying written statement explaining their rights and responsibilities. Patients and residents who receive services from an outside provider are entitled, upon request, to be told the identity of the provider. Residents shall be informed, in writing, of any health care services which are provided to those residents by individuals, corporations, or organizations other than their facility. Information shall include the name of the outside provider, the address, and a description of the service which may be rendered. In cases where it is medically inadvisable, as documented by the attending physician, advanced practice registered nurse, or physician assistant in a patient's or resident's care record, the information shall be given to the patient's or resident's guardian or other person designated by the patient or resident as a representative. Patients and residents shall have the right to respectfulness and privacy as it relates to their medical and personal care program. Case discussion, consultation, examination, and treatment are confidential and shall be conducted discreetly. Patients and residents shall be assured confidential treatment of

[44] Minnesota Statutes, Minn. Stat. § 144.296.
[45] Minnesota Statutes, Minn. Stat. § 144.293.

their personal and medical records, and may approve or refuse their release to any individual outside the facility. Residents shall be notified when personal records are requested by any individual outside the facility and may select someone to accompany them when the records or information are the subject of a personal interview. Copies of records and written information from the records shall be made available in accordance Sections 144.291 to 144.298 of the Minnesota Statutes. This right does not apply to complaint investigations and inspections by the Department of Health, where required by third-party payment contracts, or where otherwise provided by law

Minnesota Government Data Practices Act (MGDPA), Minn. Stat. Ch. 13

The MGDPA places restrictions on the disclosure of “confidential” and “private” data on individuals applies to government entities. "Government entity" means a state agency, statewide system, or political subdivision.[46]

Data Access Rules

1. Public Data on Individuals:[47] Public Data is defined as data on individuals that are not classified by state statute (including Minnesota Statutes) or federal law as private or confidential data.[48] Public Data can be accessible to anyone for any reason.

   Example: "Directory information" which includes the name of the patient, date admitted, and general condition when they are currently a patient of a hospital that is a government entity under legal commitment. After the individual is released, the information becomes private data.[49] Emergency patient directory information shall not be made public until a reasonable effort is made to next of kin or health care agent.

2. Private Data on Individuals:[50] is defined as data made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of those data.[51] Private Data shall only include data which is expressly classified by either a state statute (including the Minnesota Statutes) or federal law.[52] Private Data may be made accessible to the individual or a representative of the decedent, but may NOT be accessible to the public.
3. Confidential Data on Individuals:[53] is defined as data that is expressly classified as confidential by either a state statute (including Minnesota Statutes) or federal law.[54] Confidential Data may not be accessible to the individual or representative AND may not be accessible to the public.

[46] Minnesota Statutes, Minn. Stat. § 13.02(12).
[47] Minnesota Statutes, Minn. Stat. § 13.02(15).
[48] Minnesota Administrative Rules, Minn. R. 1205 §1205.0200(10).
[49] Minnesota Statutes, Minn. Stat. § 13.384(1).
[50] Minnesota Statutes, Minn. Stat. § 13.02(12).
[51] Minnesota Statutes, Minn. Stat. § 13.02.
[52] Minnesota Administrative Rules, Minn. R. 1205 §1205.0200(9).
[53] Minnesota Statutes, Minn. Stat. § 13.02(3).
[54] Minnesota Administrative Rules, Minn. R. 1205 §1205.0200(3).

Access to Private Data on Individuals[55]

Private Data may only be disclosed to: (i) the individual, (ii) individuals within the entity whose work assignments reasonably require access, (iii) entities and agencies as determined by the responsible authority who are authorized by Minnesota Statute or federal law to gain access to that specific data; and (iv) entities or individuals given access by the express written direction of the individual. Please note there are special rules for access to Private Data of Minors (see Minnesota Administrative Rules, Minn. R. 1205, § 1205.0500(2)).

Government Entity Obligations

1. Data inventory.[56] The designated responsible authority, which may be the Privacy Officer, shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the entity. Forms used to collect private and confidential data may be included in the inventory. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory. The inventory must be available from the responsible authority to the public. The commissioner may require responsible authorities to submit copies of the inventory and may request additional information relevant to data collection practices, policies, and procedures.

2. Public data access policy.[57] The responsible authority shall prepare a written data access policy and update it no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel, procedures, or other circumstances that impact the public's ability to access data.

3. Data subject rights and access policy.[58] The responsible authority shall prepare a written policy of the rights of data subjects under section 13.04 and the specific procedures used by the government entity for access by the data subject to public or private data on individuals. The written policy must be updated no later than August 1 of each year, and at any other time as necessary to reflect changes in personnel, procedures, or other circumstances that impact the public's ability to access data.

4. Availability.[59] The responsible authority shall make copies of the public data access policy and data subject rights and access policy easily available to the public by distributing free copies to the public or by posting the policies in a conspicuous place within the government entity that is easily accessible to the public or by posting it on the government entity's website.

[55] Minnesota Administrative Rules, Minn. R. 1205 § 1205.0400(2).
[56] Minnesota Statutes, Minn. Stat. § 13.025(1).
[57] Minnesota Statutes, Minn. Stat. § 13.025(2).
[58] Minnesota Statutes, Minn. Stat. § 13.025(3).
[59] Minnesota Statutes, Minn. Stat. § 13.025(4).

5. General standards for collection and storage.[60] Collection and storage of all data on individuals and the use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government.

6. Limitations on collection and use of data.[61] Private or confidential data on an individual shall not be collected, stored, used, or disseminated by government entities for any purposes other than those stated to the individual at the time of collection in accordance with notice requirements under the MGDPA, except in the following instances noted below.

   (a) Data collected prior to August 1, 1975, and which have not been treated as public data, may be used, stored, and disseminated for the purposes for which the data was originally collected or for purposes which are specifically approved by the commissioner as necessary to public health, safety, or welfare.

   (b) Private or confidential data may be used and disseminated to individuals or entities specifically authorized access to that data by state, local, or federal law enacted or promulgated after the collection of the data.

   (c) Private or confidential data may be used and disseminated to individuals or entities subsequent to the collection of the data when the responsible authority maintaining the data has requested approval for a new or different use or dissemination of the data and that request has been specifically approved by the commissioner as necessary to carry out a function assigned by law.

   (d) Private data may be used by and disseminated to any person or entity pursuant to the individual's informed consent.

   (e) Private or confidential data on an individual may be discussed at a meeting open to the public to the extent provided in Minnesota Statutes, Minn. Stat. § 13D.05.

7. Data protection.[62] The responsible authority shall: (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; (2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and (3) develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law. When public

[60] Minnesota Statutes, Minn. Stat. § 13.05(3).
[61] Minnesota Statutes, Minn. Stat. § 13.05(4).
[62] Minnesota Statutes, Minn. Stat. § 13.05(5).

data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.

8. Contracts.[63] Contracts between government entities and third parties must ensure that the party receiving data maintains the data in compliance with the MGDPA.

9. Preparation of summary data.[64] The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person if the request is in writing and the cost of preparing the summary data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data (1) to the administrative officer responsible for any central repository of summary data; or (2) to a person outside of the entity if the person's purpose is set forth, in writing, and the person agrees not to disclose, and the entity reasonably determines that the access will not compromise private or confidential data on individuals.

10. Intergovernmental access of data.[65] A responsible authority shall allow another responsible authority access to data classified as not public only when the access is authorized or required by statute or federal law. An entity that supplies government data under this subdivision may require the requesting entity to pay the actual cost of supplying the data.

11. International dissemination.[66] No government entity shall transfer or disseminate any private or confidential data on individuals to the private international organization known as Interpol, except through the Interpol-United States National Central Bureau, United States Department of Justice.

12. Privatization.[67] If a government entity enters into a contract with a private person to perform any of its functions, all of the data created, collected, received, stored, used, maintained, or disseminated by the private person in performing those functions is subject to the requirements of the MGDPA and the private person must comply with those requirements as if it were a government entity. All contracts entered into by a government entity must include a notice that the requirements of this subdivision apply to the contract.

13. Identification or justification.[68] Unless specifically authorized by statute, government entities may not require persons to identify themselves, state a reason for, or justify a request to gain access to public government data. A person may be asked to provide certain identifying or clarifying information for the sole purpose of facilitating access to the data.

[63] Minnesota Statutes, Minn. Stat. § 13.05(6).
[64] Minnesota Statutes, Minn. Stat. § 13.05(7).
[65] Minnesota Statutes, Minn. Stat. § 13.05(9).
[66] Minnesota Statutes, Minn. Stat. § 13.05(10).
[67] Minnesota Statutes, Minn. Stat. § 13.05(11).
[68] Minnesota Statutes, Minn. Stat. § 13.05(12).

Please see the Minnesota Administrative Rules § 1205.1300 for further information on the respective duties of the government entity.

Individual Rights

1. Tennessen warning (Privacy Notice).[69] An individual asked to supply private or confidential data concerning the individual shall be informed of: (a) the purpose and intended use of the requested data within the collecting government entity; (b) whether the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from supplying or refusing to supply private or confidential data; and (d) the identity of other persons or entities authorized by state or federal law to receive the data (for example, "all notices should include that data may be shared upon court order or provided to the state or legislative auditor"[70]).

2. Access to data by individual.[71] Upon request to a responsible authority or designee, an individual shall be informed whether the individual is the subject of stored data on individuals, and whether it is classified as public, private, or confidential. Upon further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge and, if desired, shall be informed of the content and meaning of that data. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected or created. The responsible authority or designee shall provide copies of the private or public data upon request by the individual subject of the data. The responsible authority or designee may require the requesting person to pay the actual costs of making and certifying the copies. The responsible authority or designee shall comply immediately, if possible, with any request made pursuant to this subdivision, or within ten days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. The responsible authority shall not charge the data subject any fee in those instances where the data subject only desires to view private data. The responsible authority may charge the data subject a reasonable fee for providing copies of private data.[72]

3. Procedure when data is not accurate or complete.[73] (a) An individual subject of the data may contest the accuracy or completeness of public or private data about themselves. (b) To exercise this right, an individual shall notify in writing the responsible authority of the government entity that maintains the data, describing the nature of the disagreement. (c) Upon receiving notification from the data subject, the responsible authority shall within 30 days 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

[69] Minnesota Statutes, Minn. Stat. § 13.04(2).
[70] https://mn.gov/admin/data-practices/data/warnings/tennessen/.
[71] Minnesota Statutes, Minn. Stat. § 13.04(3).
[72] Minnesota Administrative Rules, Minn. R. 1205 § 1205.0400(5).
[73] Minnesota Statutes, Minn. Stat. § 13.04(4).

individual that the responsible authority has determined the data to be correct. If the challenged data are determined to be accurate or complete, the responsible authority shall inform the individual of the right to appeal the determination to the Minnesota commissioner. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data. A data subject may appeal the determination of the responsible authority pursuant to the provisions of the Administrative Procedure Act relating to contested cases. Please see Minnesota Statutes, Minn. Stat. § 13.04(4) for more information on the appeal process.

APPENDIX II

FORMS

APPENDIX II

FORM 1

CONFIDENTIALITY AGREEMENT

EMPLOYEE CONFIDENTIALITY AGREEMENT

As an employee of Clay County, you may have access to or become aware of information that is considered confidential in nature. This information includes but is not limited to employee information, patient information, and other client information. Clay County must abide by certain Federal and state laws that protect this information. Accordingly, to protect Confidential Information that may be disclosed, the EMPLOYEE agrees as follows.

EMPLOYEE will hold the Confidential Information received during the course of employment at Clay County in strict confidence and shall exercise a reasonable degree of care to prevent disclosure to others.

EMPLOYEE will not disclose or divulge either directly or indirectly the Confidential Information to others unless first authorized to do so in writing by Clay County.

EMPLOYEE will not reproduce the Confidential Information nor use this for any purpose other than the performance of his/her duties for Clay County.

EMPLOYEE will, upon the request or upon termination of his/her relationship with Clay County, deliver to Clay County any notes, documents, equipment, and materials received from Clay County or originating from its activities for Clay County.

Clay County reserves the right to take disciplinary action, up to and including termination for violations of this agreement.

Signing below signifies that the EMPLOYEE agrees to the terms and conditions of the agreement stated above.

_____

Print Name

_____

EMPLOYEE Signature

_____

Date

APPENDIX II

FORM 2

AUTHORIZATION TO RELEASE INFORMATION

DEPARTMENT OF HUMAN SERVICES

DHS-2243A-ENG

CHILDREN AND FAMILY SERVICES - ECONOMIC ASSISTANCE AND EMPLOYMENT SUPPORTS

General Authorization for Release of Information

***IMPORTANT:** If you are not able to complete this form online, click Print Blank Form to print the form and complete it by hand.

Print Blank Form

Date: [date]

Case number: [case number]

Worker name: [first name] [last name] Worker phone: [phone number] Worker fax: [fax number]

Agency name: [agency name]

Agency address:

[street address]

To: [name]

[street address]

[city], [state] [zip code]

We need to verify information for the person(s) listed below:

PERSON'S NAME	SOCIAL SECURITY NUMBER

Add name

Please provide the information requested. **Attach verification documents *or* record the information on the back of this form and sign where indicated.** Return the form to the requesting agency. On the bottom half of this form is a signed authorization to release information to the human services agency listed above.

Thank you for your cooperation.

Authorization for release of information

Giving Permission: I give permission for the person/organization above to release the requested information to the above agency. This information is used to figure my eligibility for public assistance and/or services.

Consequences: State and Federal privacy laws protect my records. I know:

- Why I am being asked to release this information
- I do not have to consent to this authorization, but it may affect my benefits or services if I do not give my consent

- That, generally, I must give my written consent for this person/agency to give out this information, but if I do not consent, the information will not be released unless the law otherwise allows it
- I may stop this authorization with a written notice at any time, but this written notice will not affect information the agency has already requested
- The person or agency who gets my information may be able to pass it on to others
- If my information is passed on to others by DHS, it may no longer be protected by this

authorization. This authorization will end one year from the date I sign it, unless the law allows for a longer period.

CLIENT SIGNATURE	DATE	Original copy for agency Provide copy to client
SIGNATURE OF SPOUSE/GUARDIAN/AUTHORIZED REPRESENTATIVE	DATE	

CASE NUMBER: _____

To be completed by verifying agent

(Mail or fax to agency address/fax number on first page)

VERIFYING AGENT'S	
PHONE NUMBER	DATE

Attention. If you need free help interpreting this document, ask your worker or call the number below for your language.

ያስተውሉ: ይህንን ዶኩመንት ለመተርጎም እርዳታ የሚፈልጉ ከሆነ: የጉዳዮን ሰራተኛ ይጠይቁ ወይም በሰልክ ቁጥር 1-844-217-3547 ይደውሉ።

ملاحظة: إذا أردت مساعدة مجانية لترجمة هذه الوثيقة، اطلب ذلك من مشرفك أو اتصل على الرقم 1-800-358-0377.

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ပေးခြင်း အကူအညီလိုအပ်ပါက၊ သင့်လူမှုရေးအလုပ်သမား အားမေးမြန်း ခြင်းသို့ မဟုတ် 1-844-217-3563 ကိုခေါ်ဆိုပါ။

កំណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមសួរអ្នកកាន់សំណុំរឿង របស់អ្នក ឬហៅទូរស័ព្ទមកលេខ 1-888-468-3787 ។

請注意，如果您需要免費協助傳譯這份文件，請告訴您的工作人員或撥打 1-844-217-3564。

Attention. Si vous avez besoin d’une aide gratuite pour interpréter le présent document, demandez à votre agent chargé du traitement de cas ou appelez le 1-844-217-3548.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces nug koj tus neeg lis dej num los sis hu rau 1-888-486-8377.

ဟ်သူဉ်ဟ်သးဘဉ်တက့်. ဖဲနမ့်လိဉ်ဘဉ်တ်မၤစၢၤကလီလၢတ်ကကျိးထံဝဲဒဉ်လ်ာ် တီလ်ာ်မီတခါဖံၤန္ဉ်,သံကွါဘဉ်ပှၤဂ့ၢ်ဝီဒးပှၤမၤစၢၤတ်လၢနဂီၢ်မ့တမ့်ကီးဘဉ် 1-844-217-3549 တက့်.

알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 담당자에게 문의하시거나 1-844-217-3565으로 연락하십시오.

ໂປຣດຊາບ. ຖ້າຫາກ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງຖາມພະນັກງານກ່ຽວກັບການຊ່ວຍເຫຼືອ ຂອງທ່ານ ຫຼື ໂທຣໄປທີ່ 1-888-487-8251.

Hubachiisa. Dokumentiin kun bilisa akka siif hiikamu gargaarsa hoo feete, hojjettoota kee gaafadhu ykn afaan ati dubbattuuf bilbilli 1-888-234-3798.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, обратитесь к своему социальному работнику или позвоните по телефону 1-888-562-5877.

Digniin. Haddii aad u baahantahay caawimaad lacag-la’aan ah ee tarjumaadda qoraalkan, hawlwadeenkaaga weydiiso ama wac lambarka 1-888-547-8829.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, comuníquese con su trabajador o llame al 1-888-428-3438.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi nhân viên xã hội của quý vị hoặc gọi số 1-888-554-8759.

LB1 (8-16)

ADA Advisory

For accessible formats of this information, ask your county worker. For assistance with additional equal access to human services, contact your countv's ADA coordinator. ADA4 (2-18)

Authorization for Chemical Dependency Program Services

☑ Show DHS Form Version

AUTHORIZATION FOR RELEASE OF INFORMATION

Clay County Social Services - Chemical Dependency Unit 715 North 11th Street, Suite 502, Moorhead MN 56560

1 CLIENT	**FULL LEGAL NAME:**_____ **DOB:**_____ **PREVIOUS NAME:** _____
2 RELEASE INFORMATION FROM (who has the information you would like released)	☐ **Clay County Social Services, Behavioral Health Services, 715 N 11th ST, STE 502, Moorhead, MN 56560** ☐
3 RELEASE/DISCLOSE INFORMATION TO (send information to)	☐ **Clay County Social Services, Behavioral Health Services, 715 N 11th ST, STE 502, Moorhead, MN 56560** ☐
4 INFORMATION TO BE OBTAINED OR DISCLOSED ABOUT THE CLIENT NAMED ABOVE IN BOX 1 (only the information check marked will be released	**Dates of Service: From**_____**to**_____***Information from the past 12 months will be released unless dates are specified.** ☐ **Admission Summary** ☐ **Comprehensive Assessment** ☐ **Recommendations** ☐ **Discharge Summary** ☐ **DOC/Probation Records** ☐ **Diagnostic Assessment** ☐ **Progress Notes/Reports** ☐ **Court Records** ☐ **CD Tx Plans** ☐ **Lab Reports** ☐ **Dept. of Public Safety Records -MN** ☐ **Mental Health Tx Plans** ☐ **Contact Notes** ☐ **Dept. of Transportation Records- ND** ☐ **Social History/Physical** ☐ **Collateral Info from:**_____**(Name of Person)** ☐ **Other:**
5 SPECIAL DISCLOSURES	☐ **Alcohol and/or Drug Abuse/ Records** ☐ **Psychiatric and/or Mental Health** ☐ **HIV** ☐ **From**_____**to**_____**concerning**_____**(specific diagnosis or tx)** ☐ **Verbal discussion only—Do Not Release written records**
6 REASON FOR DISCLOSURE	**Release of private data and/or consent to contact collateral source for:** **Service Coordination** ☐ **Comprehensive Assessment** ☐ **Monitoring for Court** ☐ **Disability Determination** ☐ **Referrals for Treatment Placement** ☐ **Determine eligibility for services** ☐ **Other: Case management**
7 REVOCATION	**This authorization is subject to revocation at any time except to the extent that the program which is to make the disclosure has already taken action in reliance on it. If not previously revoked, this consent will terminate upon** _____**(date) or, if no date or event is specified, 12 months from the date of signing. A photocopy or fax of this authorization will be treated in the same manner as an original.** **Expired, deficient, or false consent. A disclosure may not be made on the basis of a consent which:** **(1) Has expired;** **(2) On its face substantially fails to conform to any of the required elements in CFR42;** **(3) Is known to have been revoked; or** **(4) Is known, or through a reasonable effort could be known, by the person holding the records to be materially false.**

8 **AUTHORIZATION**	**I give permission for the person/organization above to release the requested information to the above agency. I know:** • **Why I am being asked to release this information, who will receive this information and any known consequences of this release** • **That my records can be released only if I give written permission or if the law allows it** • **That if I refuse to sign or cancel this release, I may not be eligible to receive the service I am requesting** • **That the information to be released is private and any subsequent use and release is controlled under the Minnesota Government Data Practices Act and Code of Federal Regulations(CFR) 42, parts 2.31** **_____ _____** **Client Signature** **Date** **_____ _____** **Signature of Person Authorized to Consent in Lieu of Person (where required)** **Date** **☐ Parent of Minor ☐Guardian ☐Other personal representation(explain)**

Authorization for Disability Services, Long-Term Services and Support, and CHILDREN AND FAMILY SERVICES

Minnesota Department of **Human Services**

DHS-3377-ENG 9-11

Social Services Authorization for Release of Information

I, _____ authorize
(Name of individual authorizing release*)

_____

(Name of individual or entity maintaining data about me or dependent family members)

to disclose private data about me to _____.
(Name of individual(s), or entities to receive the information)

*Provide the following information if required to identify this individual from other similar names in agencies' files:				
ADDRESS				CLIENT NUMBER
CITY		STATE	ZIP CODE	SOCIAL SECURITY NUMBER
BIRTH DATE	OTHER IDENTIFYING INFORMATION			

Provide the following information:

- ☐ Discharge or closing summary
- ☐ Laboratory reports - List:
- ☐ Medical history/physical exam
- ☐ Social service records
- ☐ Progress reports
- ☐ Treatment records
- ☐ Emergency room reports
- ☐ Admission/intake summary/diagnostic Assessment
- ☐ Psychiatric evaluation
- ☐ Social history
- ☐ Psychological testing or evaluation
- ☐ Treatment plan or community support plan
- ☐ Birth records
- ☐ School records, IEP, assessments, transcripts
- ☐ Immunization records
- ☐ Vocational reports
- ☐ Medication records
- ☐ Court records
- ☐ Chemical dependency evaluation
- ☐ Other:

The information is required to:

- ☐ Continue evaluation or treatment
- ☐ Coordinate services
- ☐ Determine eligibility for case management services
- ☐ Other:

_____

Consequences: State and Federal privacy laws protect my records. I know:

- Why I am being asked for this information
- I do not have to consent to this authorization, but it may affect my benefits or services if I do not give my consent.
- That generally, I must give my written consent for this person/agency to give out this information, but if I do not consent, the information will not be shared/released unless the law otherwise allows it
- I may stop this authorization with written notice at any time, but that this written notice will not affect information the agency has already shared/requested.
- The person or agency who gets my information may be able to pass it on to others.
- If my information is passed on to others by DHS, it may no longer be protected by this authorization.

Social Services Authorization for Release of Information

This authorization ends _____, or one year from the date I sign it, unless the law allows for a longer period.
(date)

SIGNATURE OF INDIVIDUAL AUTHORIZING RELEASE	DATE
SIGNATURE OF WITNESS (if required)	DATE
SIGNATURE AND RELATIONSHIP OF PARENT, GUARDIAN OR AUTHORIZED REPRESENTATIVE (if required)	DATE

Note to agencies using this form: Prior to having this form signed you must communicate the consequences of giving informed consent to the individual. Provide a signed (executed) copy of the authorization to the individual who consents to release personal information.

Attention. If you need free help interpreting this document, ask your worker or call the number below for your language.

ያስተውሉ: ይህንን ዶኩመንት ለመተርጎም እርዳታ የሚፈልጉ ከሆነ: የጉዳዮን ሰራተኛ ይጠይቁ ወይም በሰልክ ቁጥር 1-844-217-3547 ይደውሉ።

ملاحظة: إذا أردت مساعدة مجانية لترجمة هذه الوثيقة، اطلب ذلك من مشرفك أو اتصل على الرقم 1-800-358-0377.

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ပေးခြင်း အကူအညီလိုအပ်ပါက၊ သင့်လူမှုရေးအလုပ်သမား အားမေးမြန်း ခြင်းသို့ မဟုတ် 1-844-217-3563 ကိုခေါ်ဆိုပါ။

កំណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមសួរអ្នកការន៍សំណុំរឿង របស់អ្នក ឬហៅទូរស័ព្ទមកលេខ 1-888-468-3787 ។

請注意，如果您需要免費協助傳譯這份文件，請告訴您的工作人員或撥打 1-844-217-3564。

Attention. Si vous avez besoin d'une aide gratuite pour interpréter le présent document, demandez à votre agent chargé du traitement de cas ou appelez le 1-844-217-3548.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces nug koj tus neeg lis dej num los sis hu rau 1-888-486-8377.

ဟ်သူဉ်ဟ်သးဘဉ်တက့်. ဖဲနမ့်လိဉ်ဘဉ်တ်မၤစၢၤကလီလၢတ်ကကျိးထံဝဲဒဉ်လ်ာ် တီလ်ာ်မီတခါဆံၤနှဉ်,သံကွါဘဉ်ပှၤဂ့ၢ်ဝီဒးဘပှၤမၤစၢၤတ်လၢနကိ်ာ်မ့တမ့်ကီးဘဉ် 1-844-217-3549 တက့်.

알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 담당자에게 문의하시거나 1-844-217-3565으로 연락하십시오.

ໂປຣດຊາບ. ຖ້າຫາກ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງຖາມພະນັກງານກ່ຽວກັບການຊ່ວຍເຫຼືອ ຂອງທ່ານ ຫຼື ໂທຣໄປທີ່ 1-888-487-8251.

Hubachiisa. Dokumentiin kun bilisa akka siif hiikamu gargaarsa hoo feete, hojjettoota kee gaafadhu ykn afaan ati dubbattuuf bilbilli 1-888-234-3798.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, обратитесь к своему социальному работнику или позвоните по телефону 1-888-562-5877.

Digniin. Haddii aad u baahantahay caawimaad lacag-la'aan ah ee tarjumaadda qoraalkan, hawlwadeenkaaga weydiiso ama wac lambarka 1-888-547-8829.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, comuníquese con su trabajador o llame al 1-888-428-3438.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi nhân viên xã hội của quý vị hoặc gọi số 1-888-554-8759.

LBI (8-16)

ADA5 (5-09)

This information is available in alternative formats to individuals with disabilities by calling your county worker. TTY users can call through Minnesota Relay at (800) 627-3529. For Speech-to-Speech, call (877) 627-3848. For additional assistance with legal rights and protections for equal access to human services programs, contact your agency's ADA coordinator.

APPENDIX II

FORM 3

CLAY COUNTY HIPAA AUTHORIZATION FOR TEXT MESSAGING

Clay County

HIPAA AUTHORIZATION FOR TEXT MESSAGING

As Clay County (“Clay County”) would like to ensure that it is acting in accordance with your wishes, using your personal information with your authorization, and communicating with you in a manner with which you authorize, we ask you to fill out and sign this form. Clay County will keep a copy of your written permission on file.

There may be times when you wish to communicate with Clay County personnel via text messaging. Text messages sent via standard SMS/apple iMessage are not encrypted or secured. This means that text messages could be intercepted and read by a third party.

Clay County personnel will not engage in text messaging unless you complete the form below:

I specifically authorize text messaging communication with Clay County personnel. The phone numbers I want text communications sent to are those listed below, any phone number(s) which I provide directly, or any phone numbers from which I text that prompt a response. I understand that text message communications may be unsecured. I understand that a risk of unsecured text messages is the potential that the communication could be read by a third party and further compromised. I understand my mobile provider's standard rates for sending and receiving text messages will apply.

I am not required to sign this authorization. Clay County does not condition services on the signing of this form. I can request a copy of this authorization be mailed to me. I understand that I may revoke or withdraw this authorization at any time to prohibit future use of my information. To do so, I must send written notice to Clay County Social Services Director, 715 11th St N, Suite 502, Moorhead, MN 56560. I understand that Clay County, as well as other persons or entities, may retain copies of any electronic communications or printed versions and may retain these versions forever. Any revocation of this authorization will only extend to the versions of the information within my control that have not been previously published. If not revoked/withdrawn by me, this authorization expires as of the date my case is closed.

Name: _____
Signature: _____ Date: _____
Address: _____ (street address)
_____ (city) (state) (zip code)

Parent/Guardian Name:_____

Parent/Guardian Signature:_____

Phone Number(s): _____

APPENDIX II

FORM 4

PRIVACY NOTICE ACKNOWLEDGEMENT AND CONSENT TO THE USE AND DISCLOSURE OF PERSONAL HEALTH INFORMATION

Clay County

Privacy Notice Acknowledgement and

Consent to the Use and Disclosure of Personal Health Information

I,_____**,** understand and agree that Clay County may use and disclose protected health information (including but not limited to name, address, health history, symptoms, examination and test results, diagnosis and treatment) for treatment, payment or health care operations. I also understand that this does not preclude any existing federal or state confidentiality regulations applying to this program that may be more restrictive with regard to release of confidential client information.

I understand and have been provided a copy of the document entitled Notice of Privacy Practices which provides a complete description of potential uses and disclosures of my protected health information. I understand that I have the right to review the Notice of Privacy Practices prior to signing the consent.

I understand that Clay County reserves the right to change its privacy practices and will immediately post the changes and provide me a copy of any revised notice at my request.

I understand that I have the right to request that Clay County restrict how my protected health information is used or disclosed to carry out treatment, payment, or health care operation. I further understand that Clay County is not required to grant any request to restrict the use or disclosure of information.

If, however, Clay County agrees to a requested restriction, the restriction is binding on Clay County.

Signature _____Date _____

Printed Name _____

Witness Signature _____Date _____

Printed Name _____

☐ Individual refused to acknowledge receipt of Privacy Notice

Clay County Employee Signature, _____

Printed Name_____

Title _____Date _____

Clay County Social Services Director, 715 11th St N, Suite 502, Moorhead, MN 56560

Clay County Chemical Health – Client Forms Checklist

Client Name: Date of Assessment:

☐ I have been offered a copy of "***Notice of Privacy Practices***"

☐ Accepted copy ☐ Declined copy

☐ I have reviewed the "***Confidentiality of Alcohol and Drug Abuse Client Records***" and the "***Right to Second Assessments and Client's Rights to Appeal Notice"***

☐ Accepted copy ☐ Declined copy

My signature indicates that I have had the above information given and/or explained to me.

_____ _____

Client Signature Date

Clay County Social Services Worker or Clay County Representative

APPENDIX II

FORM 5

NOTICE OF PRIVACY PRACTICES

DHS-3979-ENG 11-16

Notice of Privacy Practices

(Effective Date: November 2016)

This notice tells how private information about you may be used and disclosed and how you can get this information. Please review it carefully.

Why do we ask for this information?

• In order to determine whether and how we can help you, we collect information:
• To tell you apart from other people with the same or similar name
• To decide what you are eligible for
• To help you get medical, mental health, financial or social services and decide if you can pay for some services
• To decide if you or your family need protective services
• To decide about out-of-home care and in-home care for you or your children
• To investigate the accuracy of the information in your application
• After we have begun to provide services or support to you, we may collect additional information:
• To make reports, do research, do audits, and evaluate our programs
• To investigate reports of people who may lie about the help they need
• To collect money from other agencies, like insurance companies, if they should pay for your care
• To collect money from the state or federal government for help we give you.
• When your or your family's circumstances change and you are required to report the change (see Client Responsibilities and Rights – DHS-4163)

Why do we ask you for your Social Security number?

We need your Social Security number to give you medical assistance, some kinds of financial help, or child support enforcement services (42 CFR 435.910 [2006]; Minn. Stat. 256D.03, subd.3(h); Minn. Stat.256L.04, subd. 1a; 45 CFR 205.52 [2001]; 42 USC 666; 45 CFR 303.30 [2001]). We also need your Social Security Number to verify identity and prevent duplication of state and federal benefits. Additionally, your Social Security Number is used to conduct computer data matches with collaborative, nonprofit and private agencies to verify income, resources, or other information that may affect your eligibility and/or benefits.

You do not have to give us the Social Security Number:

• For persons in your home who are not applying for coverage
• If you have religious objections
• If you are not a United States citizen and are applying for Emergency Medical Assistance only
• If you are from another country, in the United States on a temporary basis and do not have permission from the United States Citizenship and Immigration Services to live in the United States permanently
• If you are living in the United States without the knowledge or approval of the U.S. Citizenship and Immigration Services.

Do you have to answer the questions we ask?

You do not have to give us your personal information. Without the information, we may not be able to help you. If you give us wrong information on purpose, you can be investigated and charged with fraud.

With whom may we share information?

We will only share information about you as needed and as allowed or required by law. We may share your information with the following agencies or persons who need the information to do their jobs:

• Employees or volunteers with other state, county, local, federal, collaborative, nonprofit and private agencies
• Researchers, auditors, investigators, and others who do quality of care reviews and studies or commence prosecutions or legal actions related to managing the human services programs.
• Court officials, county attorney, attorney general, other law enforcement officials, child support officials, and child protection and fraud investigators
• Human services offices, including child support enforcement offices
• Governmental agencies in other states administering public benefits programs
• Health care providers, including mental health agencies and drug and alcohol treatment facilities
• Health care insurers, health care agencies, managed care organizations and others who pay for your care

• Guardians, conservators or persons with power of attorney
• Coroners and medical investigators if you die and they

What privacy rights do children have?

investigate your death
• Credit bureaus, creditors or collection agencies if you do not pay fees you owe to us for services
• Anyone else to whom the law says we must or can give the information.

What are your rights regarding the information we have about you?

• You and people you have given permission to may see and copy private information we have about you. You may have to pay for the copies.

• You may question if the information we have about you is correct. Send your concerns in writing. Tell us why the information is wrong or not complete. Send your own explanation of the information you do not agree with. We will attach your explanation any time information is shared with another agency.

• You have the right to ask us in writing to share information with you in a certain way or in a certain place. For example, you may ask us to send health information to your work address instead of your home address. If we find that your request is reasonable, we will grant it.

• You have the right to ask us to limit or restrict the way that we use or disclose your information, but we are not required to agree to this request.

• If you do not understand the information, ask your worker to explain it to you. You can ask the Minnesota Department of Human Services for another copy of this notice.

What are our responsibilities?

• We must protect the privacy of your private information according to the terms of this notice.

• We may not use your information for reasons other than the reasons listed on this form or share your information with individuals and agencies other than those listed on this form unless you tell us in writing that we can.

• We must follow the terms of this notice, but we may change our privacy policy because privacy laws change. We will put changes to our privacy rules on our website at: http://edocs.dhs.state.mn.us/lfserver/Public/DHS-3979-ENG

If you are under 18, when parental consent for medical treatment is not required, information will not be shown to parents unless the health care provider believes not sharing the information would risk your health. Parents may see other information about you and let others see this information, unless you have asked that this information not be shared with your parents. You must ask for this in writing and say what information you do not want to share and why. If the agency agrees that sharing the information is not in your best interest, the information will not be shared with your parents. If the agency does not agree, the information may be shared with your parents if they ask for it.

What if you believe your privacy rights have been violated?

If you think that the Minnesota Department of Human Services has violated your privacy rights, you may send a written complaint to the U.S. Department of Health and Human Services to the address below: Minnesota Department of Human Services Attn: Privacy Official PO Box 64998 St. Paul, MN 55164-0998

Attention. If you need free help interpreting this document, ask your worker or call the number below for your language.

ያስተውሉ፡ ይህንን ዶኩመንት ለመተርጎም እርዳታ የሚፈልጉ ከሆነ፡ የጉዳዮን ሰራተኛ ይጠይቁ ወይም በሰልክ ቁጥር 1-844-217-3547 ይደውሉ።

ملاحظة: إذا أردت مساعدة مجانية لترجمة هذه الوثيقة، اطلب ذلك من مشرفك أو اتصل على الرقم 1-800-358-0377.

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ပေးခြင်း အကူအညီလိုအပ်ပါက၊ သင့်လူမှုရေးအလုပ်သမား အားမေးမြန်း ခြင်းသို့ မဟုတ် 1-844-217-3563 ကိုခေါ်ဆိုပါ။

កំណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមសួរអ្នកកាន់សំណុំរឿង របស់អ្នក ឬហៅទូរស័ព្ទមកលេខ 1-888-468-3787 ។

請注意，如果您需要免費協助傳譯這份文件，請告訴您的工作人員或撥打 1-844-217-3564。

Attention. Si vous avez besoin d’une aide gratuite pour interpréter le présent document, demandez à votre agent chargé du traitement de cas ou appelez le 1-844-217-3548.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces nug koj tus neeg lis dej num los sis hu rau 1-888-486-8377.

ဟ်သူဉ်ဟ်သးဘဉ်တက့်. ဖဲနမ့်လိဉ်ဘဉ်တ်မၤစၢၤကလီလၢတ်ကကျိးထံဝဲဒဉ်လ်ာ် တီလ်ာ်မီတခါဖၣံၤန္ဉ်,သံကွ်ဘဉ်ပှၤဂ့ၢ်ဝီဒးပှၤမၤစၢၤတ်လၢနဂီၢ်မ့တမ့်ကီးဘဉ် 1-844-217-3549 တက့်.

알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 담당자에게 문의하시거나 1-844-217-3565으로 연락하십시오.

ໂປຣດຊາບ. ຖ້າຫາກ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງຖາມພະນັກງານກໍາກັບການຊ່ວຍເຫຼືອ ຂອງທ່ານ ຫຼື ໂທຣໄປທີ່ 1-888-487-8251.

Hubachiisa. Dokumentiin kun bilisa akka siif hiikamu gargaarsa hoo feete, hojjettoota kee gaafadhu ykn afaan ati dubbattuuf bilbilli 1-888-234-3798.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, обратитесь к своему социальному работнику или позвоните по телефону 1-888-562-5877.

Digniin. Haddii aad u baahantahay caawimaad lacag-la’aan ah ee tarjumaadda qoraalkan, hawlwadeenkaaga weydiiso ama wac lambarka 1-888-547-8829.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, comuníquese con su trabajador o llame al 1-888-428-3438.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi nhân viên xã hội của quý vị hoặc gọi số 1-888-554-8759.

LB1 (8-16)

ADA Advisory

For accessible formats of this information, ask your county worker. For assistance with additional equal access to human services, contact your county's ADA coordinator. ADA4 (2-18)

Chemical Dependency Program Notice of Privacy Practices

DHS-3979-ENG 11-16

Notice of Privacy Practices
(Effective Date: November 2016)

This notice tells how private information about you may be used and disclosed and how you can get this information. Please review it carefully.

Why do we ask for this information?

• In order to determine whether and how we can help you, we collect information:
• To tell you apart from other people with the same or similar name
• To decide what you are eligible for
• To help you get medical, mental health, financial or social services and decide if you can pay for some services
• To decide if you or your family need protective services
• To decide about out-of-home care and in-home care for you or your children
• To investigate the accuracy of the information in your application
• After we have begun to provide services or support to you, we may collect additional information:
• To make reports, do research, do audits, and evaluate our programs
• To investigate reports of people who may lie about the help they need
• To collect money from other agencies, like insurance companies, if they should pay for your care
• To collect money from the state or federal government for help we give you.
• When your or your family's circumstances change and you are required to report the change (see Client Responsibilities and Rights – DHS-4163)

Why do we ask you for your Social Security number?

We need your Social Security number to give you medical assistance, some kinds of financial help, or child support enforcement services (42 CFR 435.910 [2006]; Minn. Stat. 256D.03, subd.3(h); Minn. Stat.256L.04, subd. 1a; 45 CFR 205.52 [2001]; 42 USC 666; 45 CFR 303.30 [2001]). We also need your Social Security Number to verify identity and prevent duplication of state and federal benefits. Additionally, your Social Security Number is used to conduct computer data matches with collaborative, nonprofit and private agencies to verify income, resources, or other information that may affect your eligibility and/or benefits.

You do not have to give us the Social Security Number:
• For persons in your home who are not applying for coverage
• If you have religious objections
• If you are not a United States citizen and are applying for Emergency Medical Assistance only
• If you are from another country, in the United States on a temporary basis and do not have permission from the United States Citizenship and Immigration Services to live in the United States permanently
• If you are living in the United States without the knowledge or approval of the U.S. Citizenship and Immigration Services.

Do you have to answer the questions we ask?

You do not have to give us your personal information. Without the information, we may not be able to help you. If you give us wrong information on purpose, you can be investigated and charged with fraud.

With whom may we share information?

We will only share information about you as needed and as allowed or required by law. We may share your information with the following agencies or persons who need the information to do their jobs:
• Employees or volunteers with other state, county, local, federal, collaborative, nonprofit and private agencies
• Researchers, auditors, investigators, and others who do quality of care reviews and studies or commence prosecutions or legal actions related to managing the human services programs.
• Court officials, county attorney, attorney general, other law enforcement officials, child support officials, and child protection and fraud investigators
• Human services offices, including child support enforcement offices
• Governmental agencies in other states administering public benefits programs
• Health care providers, including mental health agencies and drug and alcohol treatment facilities
• Health care insurers, health care agencies, managed care organizations and others who pay for your care
• Guardians, conservators or persons with power of attorney
• Coroners and medical investigators if you die and they investigate your death
• Credit bureaus, creditors or collection agencies if you do not pay fees you owe to us for services

What privacy rights do children have?

If you are under 18, when parental consent for medical treatment is not required, information will not be shown to parents unless the health care provider believes not sharing the information would risk your health. Parents may see other information about you and let others see

• Anyone else to whom the law says we must or can give the information.

What are your rights regarding the information we have about you?

• You and people you have given permission to may see and copy private information we have about you. You may have to pay for the copies.
• You may question if the information we have about you is correct. Send your concerns in writing. Tell us why the information is wrong or not complete. Send your own explanation of the information you do not agree with. We will attach your explanation any time information is shared with another agency.
• You have the right to ask us in writing to share information with you in a certain way or in a certain place. For example, you may ask us to send health information to your work address instead of your home address. If we find that your request is reasonable, we will grant it.
• You have the right to ask us to limit or restrict the way that we use or disclose your information, but we are not required to agree to this request.
• If you do not understand the information, ask your worker to explain it to you. You can ask the Minnesota Department of Human Services for another copy of this notice.

What are our responsibilities?

• We must protect the privacy of your private information according to the terms of this notice.
• We may not use your information for reasons other than the reasons listed on this form or share your information with individuals and agencies other than those listed on this form unless you tell us in writing that we can.
• We must follow the terms of this notice, but we may change our privacy policy because privacy laws change. We will put changes to our privacy rules on our website at: http://edocs.dhs.state.mn.us/lfserver/Public/DHS-3979-ENG

this information, unless you have asked that this information not be shared with your parents. You must ask for this in writing and say what information you do not want to share and why. If the agency agrees that sharing the information is not in your best interest, the information will not be shared with your parents. If the agency does not agree, the information may be shared with your parents if they ask for it.

What if you believe your privacy rights have been violated?

If you think that the Minnesota Department of Human Services has violated your privacy rights, you may send a written complaint to the U.S. Department of Health and Human Services to the address below: Minnesota Department of Human Services Attn: Privacy Official PO Box 64998 St. Paul, MN 55164-0998

Attention. If you need free help interpreting this document, ask your worker or call the number below for your language.

ያስተውሉ፡ ይህንን ዶኩመንት ለመተርጎም እርዳታ የሚፈልጉ ከሆነ፡ የጉዳዮን ሰራተኛ ይጠይቁ ወይም በሰልክ ቁጥር 1-844-217-3547 ይደውሉ።

ملاحظة: إذا أردت مساعدة مجانية لترجمة هذه الوثيقة، اطلب ذلك من مشرفك أو اتصل على الرقم 1-800-358-0377.

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ဝေးခြင်း အကူအညီလိုအပ်ပါက၊ သင့်လုပ္ကုဒေးအလုပ်သမား အားဖေးမြန်း ခြင်းသို့ မဟုတ် 1-844-217-3563 ကိုခေါ်ဆိုပါ။

ក័ណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមសួរអ្នកការងារសង្គម ឬហៅទូរស័ព្ទមកលេខ 1-888-468-3787 ។

請注意，如果您需要免費協助傳譯這份文件，請告訴您的工作人員或撥打 1-844-217-3564。

Attention. Si vous avez besoin d'une aide gratuite pour interpréter le présent document, demandez à votre agent chargé du traitement de cas ou appelez le 1-844-217-3548.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces nug koj tus neeg lis dej num los sis hu rau 1-888-486-8377.

ဟသ္ဥဟ်သးဘဉ်တကွံ. ဖဲနမ့ါလိဉ်ဘဉ်တါမၤစၢၤကလီလၢတါ်ကကျိးထံဝဲဒဉ်လာ် တိလာ်မီတခါးဆံးနှဉ်,သံကွါဘဉ်ပှၤဂ့ါဝိဒမ့ၤမၤစၢၤတါ်လၢနှဂီၢ်မ့တမ့ါကီးဘဉ် 1-844-217-3549 တကွံ.

알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 담당자에게 문의하시거나 1-844-217-3565으로 연락하십시오.

ໂປດຊາບ. ຖ້າທ່ານ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງຖາມພະນັກງານກໍາກັບການຊ່ວຍເຫຼືອ ຂອງທ່ານ ຫຼື ໂທຣໄປທີ່ 1-888-487-8251.

Hubachiisa. Dokumentiin kun bilisa akka siif hiikamu gargaarsa hoo feete, hojjettoota kee gaafadhu ykn afaan ati dubbattuuf bilbilli 1-888-234-3798.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, обратитесь к своему социальному работнику или позвоните по телефону 1-888-562-5877.

Digniin. Haddii aad u baahantahay caawimaad lacag-la'aan ah ee tarjumaadda qoraalkan, hawlwadeenkaaga weydiiso ama wac lambarka 1-888-547-8829.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, comuníquese con su trabajador o llame al 1-888-428-3438.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi nhân viên xã hội của quý vị hoặc gọi số 1-888-554-8759.

LB (4-16)

ADA Advisory

For accessible formats of this information, ask your county worker. For assistance with additional equal access to human services, contact your county's ADA coordinator. ADA4 (2-18)

CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE CLIENT RECORDS

This notice describes how medical information about you may be used/disclosed and how you can get access to this information. Please review carefully.

The privacy of alcohol and drug records maintained by this program are protected by various Federal and State laws and regulation. Among these are:

38 U.S.Code 7332-Confidentiality of Certain Medical Records
42 U.S.Code .290dd-3-Alcohol Abuse Patient Records
42 U.S.Code .290ee-3-Drug Abuse Patient Records
42 CFR Part 2-Confidentiality of Alcohol and Drug Abuse Patient Records
Minnesota Statute 13-Government Data Practices
Minnesota Statute 144.291-144.34-MN Health Records Act
Minnesota Statute 254A.09-Confidentiality of Records
Minnesota Statute-626.5561-Reporting of Prenatal Exposure to Controlled Substances
Minnesota Rules, Chapter 1205-Data Practices
Minnesota Rules, Chapter 9530-Chemical Dependency Programs

Why do we ask for this information? The information you were asked to provide will be used to identify, diagnose, plan, and provide services to you, compile statistical reports, and evaluate programs.

Do you have to answer the questions we ask? No. However, without the information, we may not be able to help you or be able to complete an assessment. The State will not pay for treatment unless you answer the questions.

With whom may we share information? Your records are private. Workers in this agency and with the Minnesota Department of Human Services have access to your records if they need it to do their jobs. (Example: Agency employees working on placement in treatment can see your records; Agency employees who arrange for payment have access to your records; Workers from the Minnesota Department of Human Services who send out treatment payments or check county records also have access to your records.) You have the right to see your record. You have the right to obtain a copy of your record. The Agency may charge you for the cost of finding the record and making copies. If you want to see the record, the agency must provide it at no cost.

Generally, the program may not say to an outside person or agency that you are receiving services UNLESS:

1. You consent in writing.
2. The disclosure is allowed by a Court Order.
3. The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation.
4. The disclosure is made pursuant to Minnesota Supreme Court ruling to report to local welfare or law enforcement agency suspected child abuse or neglect. The program is not required to obtain your written consent or other authorization under these regulations in order to provide such access to your records.
5. The disclosure is made to protect your life or the life of another.

Violation of the Federal and State law and regulations by a program is a crime. Suspected violation may be reported to appropriate authorities in accordance with Federal and State regulations.

Your records may not be used to initiate or substantiate any criminal charges against you unless that crime occurred on the premises of the program or against personnel of the program or consisted of your threat to commit such a crime.

DHS-4839E-ENG 11-22

MINNESOTA DEPARTMENT OF HUMAN SERVICES

Notice of Privacy Practices and Notice of Rights and Responsibilities

(Effective Date: November 2022)

Notice of Privacy Practices

This part of the notice describes how private or confidential information about you may be used and disclosed. Please review it carefully.

Why do we ask for this information?

- To tell you apart from other people with the same or similar name
- To decide what you are eligible for
- To help you get medical and mental health services and decide whether you can pay for some services
- To decide whether you or your family need protective services
- To decide about out-of-home care and in-home care for you or your children
- To make reports, do research, do audits, and evaluate our programs
- To investigate reports of people that may lie about the help they need or to get assistance they may not be entitled to receive
- To collect money from other agencies, like insurance companies, if they should pay for your care
- To collect money from the state or federal government for help we give you

Why do we ask you for your Social Security number?

We need your Social Security number (SSN) to give you Medical Assistance (MA), some kinds of financial help, and child support enforcement services (42 USC 666; Minn. Stat. 256L.04, subd. 1a; 42 CFR 435.910).

We also need your SSN to verify identity and prevent duplication of state and federal benefits. Additionally, your SSN is used to conduct computer data matches with our partner nonprofit and private agencies to verify income, resources, and other information that may affect your eligibility or benefits.

You do not have to give us the SSN for people in your home who are not applying for coverage. You also do not have to give us your SSN:

- If you have religious objections
- If you are not a U.S. citizen and are applying for Emergency Medical Assistance only
- If you are from another country, are in the U.S. on a temporary basis, and do not have permission from the U.S. Citizenship and Immigration Services (USCIS) to live in the U.S. permanently
- If you are living in the U.S. without the knowledge or

Why do we ask you for your financial information?

We use this information only for the purposes authorized by law, such as verifying eligibility or determining the amount of a premium. We will not share this information with any other person or entity.

Do you have to answer the questions we ask?

You do not have to give us your personal information. Without the information, we may not be able to help you. If you give us wrong information on purpose, you could be investigated and then charged with a crime.

With whom may we share information?

We will share information about you only as needed and as allowed or required by law. We may share your information with the following agencies or people who need the information to do their jobs:

- Employees or volunteers with other state, county, local, federal, and partner nonprofit and private agencies
- Researchers, auditors, investigators, and others that do quality-of-care reviews and studies or begin prosecutions or legal actions related to managing the human services programs
- Court officials, county attorneys, attorneys general, other law enforcement officials, child support officials, child protection and fraud investigators, and fraud prevention investigators
- Human services offices, including child support enforcement offices
- Governmental agencies in other states administering public benefits programs
- Health care providers, including mental health agencies and drug and alcohol treatment facilities
- Health care insurers, health care agencies, managed care organizations and others that pay for your care
- Guardians, conservators or people with power of attorney who are authorized representatives
- Coroners and medical investigators if you die and they investigate your death
- Credit bureaus, creditors or collection agencies if you do not pay fees you owe to us for services, in limited situations

approval of the USCIS

What are our responsibilities?

- We must protect the privacy of your personal, health care and other private information according to the terms of this notice.
- We may not use your information for reasons other than the reasons listed on this form or share your information with people and agencies other than those listed on this form unless you tell us in writing that we can.
- We will not sell any data collected, created, or maintained as part of thisapplication.
- We must follow the terms of this notice and give you a copy of it, but we may change our privacy policy. Those changes will apply to all information we have about you. The new notice will be available on request, and we will put changes to it on our website at https://edocs.dhs.state.mn.us/lfserver/Public/DHS-4839E-ENG.
- The law requires us to keep your private information private and secure.
- Ifsomethinghappensthatcausesyourprivateinformation to no longer be private and secure, we will let you know right away.

This part of the notice describes how medical information about you may be used and disclosed and how you can get access to this information.
Please review it carefully.

We can use and share your health care information to

- **Help manage the health care treatment you receive**
  - We can use your health information and share it with professionals who are treating you. *Example: A doctor sends us information about your diagnosis and treatment plan so we can arrange additional services.*
  - We can also share your information with guardians, conservators or people with power of attorney who are authorized representatives
- **Run our organization**
  - We can use and share your information to run our organization and contact you when necessary. This includes sharing your information with employees or volunteers with other state, county, local, federal, and partner nonprofit and private agencies, including child support offices.
  - We can share your information with these people and groups:
    - Auditors, investigators, and others that do quality-of- care reviews and studies
    - Credit bureaus, creditors or collection agencies if you do not pay fees you owe to us for services, in limited situations
    - Certified application counselors, in-person assisters, and navigators and anyone else the law says we must or can give the information to
  - We are not allowed to use genetic information to decide whether we will give you coverage and the price of that coverage. This does not apply to long-term-care plans.
- Certified application counselors, in-person assisters, and navigators and anyone else the law says we must or can give the information to
- **Pay for your health services**
  - We can use and share your health information as we pay for your health services. *Example: We share information about you with your dental plan to coordinate payment for your dental work.*
- **Help with public health and safety issues**
  - We can share health information about you for purposes such as:
    - Preventing disease
    - Helping with product recalls
    - Reporting adverse reactions to medications
    - Reporting suspected abuse, neglect, or domestic violence
    - Preventing or reducing a serious threat to anyone's health or safety
- **Do research**
  - We can use or share your information for health research.
- **Comply with the law**
  - We will share information about you if state or federal laws require it. This includes sharing information with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.
- **Respond to organ and tissue donation requests and work with a medical examiner or funeral director**
  - We can share health information about you with organ procurement organizations.
  - We can share health information with a coroner,medical examiner, or funeral director when a person dies.
- **Address workers' compensation, law enforcement, and other government requests**
  - For workers' compensation claims
  - For law enforcement purposes or with a law enforcement official
  - With health oversight agencies for activities authorized bylaw
  - With governmental agencies in other states administering public benefits programs
  - For special government functions, such as military, national security,and presidential protective services
- **Respond to lawsuits and legal actions**
  - We can share health information about you in response to a court order. We may share the information with court officials, county attorneys, attorneys general, other law enforcement officials, child support officials, child protection and fraud investigators, and fraud prevention investigators.

What are your rights regarding the information we have about you?

Get a copy of health and claims records

- You and people you have given permission to may see and copy private information we have about you, such as health and claims

Example: We use health information about you to develop better services for you.

Ask us to correct health and claims records

- You may question whether the information we have about you is correct. Send your concerns in writing. Tell us why the information is wrong or incomplete. Send your own explanation of the information you do not agree with. We **will** attach your explanation anytime information is shared.

Request confidential communications

- You have the right to ask us in writing to share health information with you in a certain way or in a certain place.
- We will consider all reasonable requests. We must say yes if you tell us you would be in danger if we did not. For example, you may ask us to send health information to your work address instead of your home address. If we find that your request is reasonable, we will grant it.

Ask us to limit what we use or share

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request and we may say no if it would affect your care.

Get a list of those with whom we've shared information

- This list will not include disclosures for treatment, payment, and health care operation s. It will also not include certain other disclosures, such as any you asked us to make.
- We'll provide one list a year for free but will charge a reasonable, cost-based fee if you ask for another one within 12 months.

Get a copy of this privacy notice

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

If you do not understand the information, ask your worker to explain it to you. You may ask the Minnesota Department of Human Services for another copy of this notice.

What are your choices?

For certain health information, you can tell us your choices about what we share.

You have both the right and choice to tell us to:

- Share health information with your family, close friends, or others involved in payment for your care
- Share information in a disaster relief situation

Tell us what you want us to do, and we will follow your instructions. If you are not able to tell us your preference, for example, if you are unconscious, we may go ahead and share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

records. You may have to pay for the copies.

- You can choose someone to act for you with a medical power of attorney or as a legal guardian. That person can exercise your rights and make choices about your information.

What privacy rights do children have?

If you are under 18, when parental consent for medical treatment is not required, information will be provided to parents only when the medical provider believes that your health is at risk if the information is not shared. Parents may see other information about you and let others see this information, unless you have asked that this information not be shared with your parents. You must ask for this in writing and say what information you do not want to share and why. If the agency agrees that sharing the information is not in your best interest, the information will not be shared with your parents. If the agency does not agree, the information may be shared with your parents if they ask for it.

What if you believe your privacy rights have been violated?

You may complain if you believe your privacy rights have been violated. You cannot be denied service or treated badly because you have made a complaint. If you believe that your medical privacy was violated by your doctor or clinic, a health insurer, a health plan, or a pharmacy, you may send a written complaint to either the county agency, the organization or the federal **civil** rights office at:

U.S. Department of Health and Human Services
Office for Civil Rights, Region V
233 N. Michigan Avenue, Suite 240
Chicago, IL 60601
312-886-2359 (voice)
800-368-1019 (toll free)
800-537-7697 (TTY)
312-886-1807 (fax)

If you believe the Minnesota Department of Human Services violated your privacy right s, you may also contact:

Minnesota Department of Human Services
Attn: Data Complaint
PO Box 64998
St. Paul, MN 55164-0998

Whom do you contact if you need more information about privacy practices?

If you need more information about privacy practices, call the Minnesota Health Care Programs (MHCP) Member Help Desk at 800-657-3739 or 651-431-2670.

Notice of Rights and Responsibilities

Changes

If you have MA, you must report a change within 10 days of the change happening. Call your county or tribal agency to report the change.

If you do not report changes, you may have to pay money back to the state or federal government for benefits that you received but were not eligible for. If you are not sure whether to report a change, call and explain what is happening. Examples of changes you need to report include the following:

Income changes when you

- Start a new job, change jobs or stop a job
- Start to get, or receive changes in the amount of, other income like Social Security, other retirement income and unemployment

Residence changes when you

- Move to a new address

Life changes in your household when someone

- Starts or stops other health insurance or Medicare
- Becomes pregnant or has a baby
- Moves in or out of your home
- Changes tax filing status
- Loses Minnesota residency
- Changes citizenship or lawful presence status
- Changes incarceration status
- Dies, gets married or gets a divorce
- Becomes disabled

Reviews

The state or federal agency's health care program auditors may look at your case. They will review the information you gave us and check to make sure we processed your case correctly. They will let you know if they need to ask you questions.

Consent for Sharing of Medical Information

In your application for Minnesota Health Care Program coverage, you have given your written and signed consent to the following agencies and people to share between them medical information about you only for the limited purposes indicated:

- Health providers, including health plans, insurance agencies, Minnesota Health Care Programs, county advocates, school districts, your county or state case workers, and their contractors and subcontractors, for these purposes:
  - To determine who should pay for your health care
  - To provide, manage and coordinate health care services
- **All** other agencies or people listed on this Notice of Privacy

This consent applies to medical information about your minor children you applied for on this application.

You can stop this consent at any time by asking in writing for it to end. The written notice to stop this consent **will** not affect information the agency has already given to others.

This consent is good while you are enrolled in Minnesota Health Care Programs, up to one year or longer if the law permits.

However, it does not end after one year for records given to consulting providers or for payment of your bills, fraud investigations or quality-of-care review and studies.

An agency or person who gets your information through this consent could give the information to others.

If you end this consent, you cannot enroll or stay enrolled in Minnesota Health Care Programs.

Other Health Care

You and your household members enrolled in MA must tell us about any other health insurance that you have or that is available to you, including employer-sponsored coverage, private health insurance, long-term-care insurance, and any limited health coverage, such as dental or accident coverage. You must tell us whether your employer offers insurance and whether you accepted it.

You and your household members enrolled in MA may need to accept and keep a health insurance policy when the policy is found to be cost effective. If you have a good reason for not doing that, you may ask the state to approve the reason. If you do not give us information about your health insurance policy, you may not get coverage.

You must also tell us when you become eligible for Medicare. MA pays for the Medicare premiums of some low-income people. Once you are eligible for Medicare Part B and Part D, MA will no longer pay for services that could be covered by a Medicare program.

MA Medical Support

If you are applying for yourself and your children and you do not live with the other parent, the law says you may have to give information to child support staff if both you and your child are eligible for MA. This includes helping the state prove who the father of your children is and helping the state to get the other parent to help pay the children's medical expenses. If you do not help child support staff, your children will still get coverage, but your coverage will end, unless you are

Practices and Notice of Rights and Responsibilities, for this purpose:

- To administer Minnesota Health Care Programs, pay for services, and conduct research and investigations

Assignment of Medical Payments

By accepting MA, you give your rights to all medical payments for yourself and anyone else you apply for to the state of Minnesota. These include medical payments from all other people or companies, including medical support payments from an absent parent. This assignment of medical payments begins as soon as health care coverage starts. For MA for Long-Term Care, this includes your right to support from your spouse under Minnesota Statutes, section 256B.14, subdivision 3.

You also agree to help the state get paid back for medical expenses that should have been paid by others. You may not have to help the state if you have a good reason for not helping and the state approves the reason.

MA Estate Claims and Liens

In certain circumstances, federal and state law require the Minnesota Department of Human Services and local agencies to recover costs that the MA program paid for its members health care services. This recovery process is done through Minnesota's MA estate recovery and lien program.

If you are enrolled in MA when you are 55 years old or older, then, after you die, Minnesota must try to recover certain payments the MA program made for your health care, including:

- Nursing home services
- Home and community-based services
- Related hospital and prescription drug costs
- Managed Care premiums (capitations) for coverage of these services

If you permanently live in a medical institution, Minnesota must also try to recover the costs of all MA services you receive at any age while living in a medical institution. If you are permanently living in a medical institution and you do not have a spouse or disabled child living on your homesteaded real property, the state may file an MA lien against your real property to recover MA costs before your death. However, MA members who qualify for services under modified adjusted gross income (MAGI) eligibility criteria are not subject to recovery for services received before the age of 55.

After you die, the state also may file a notice of potential claim, which is a form of lien, against real property to recover MA costs. Liens to recover MA costs may be filed against the following:

- Your life estate or joint tenancy interest in real property
- Your real property that you own solely
- Your real property that you own with someone else

Minnesota cannot start recovery of these costs while your spouse is still living or if you have a child under 21 years old or a child who is permanently disabled. Once your spouse dies, Minnesota must pregnant.

If you are afraid the other parent may cause harm to you or your child, you can give your county or tribal agency proof to support your fears. The agency will review your proof and tell you whether you still must give information to child support staff.

Your children do not have to use their assets to reimburse the state for any MA services you received.

You have the right to speak with a legal-aid group or a private attorney if you have specific questions about how MA estate recovery and liens may affect your circumstance and estate planning. The Minnesota Department of Human Services cannot provide you with legal advice. For more information, go to http://mn.gov/dhs/ma-estate-recovery/.

You Have the Right to Ask for a Hearing

If you feel your health care eligibility or benefits are wrong or your application was not processed correctly, you may ask for an appeal hearing. By requesting an appeal hearing, you are requesting a fair review of your case. You can represent yourself or use an attorney, advocate, authorized representative, relative, friend or other person. You will find specific appeal instructions on all eligibility notices that you receive. Learn more about the appeals process and how to ask for a hearing at www.dhs.state.mn.us/appeals/faqs.

You can complete and submit an appeal request online at https://edocs.dhs.state.mn.us/lfserver/Public/DHS-0033-ENG.

You can also print the form that is available at the address above and submit the completed form by fax to 651-431-7523 or by mail to this address:

Minnesota Department of Human Services
Appeals Division
PO Box 64941
St. Paul, MN 55164-0941

Immigration

Immigration information you give to us is private. We use it to see whether you can get coverage. We share it only when the law allows it or requires it, such as to verify identity. In most cases, applying will not affect your immigration status unless you are applying for payment of long-term-care services.

You do not have to give us your immigration information if you are a pregnant woman living in the United States without the knowledge or approval of the United States Citizenship and Immigration Services (USCIS). You also do not have to give us your immigration information if you are:

- Applying for emergency medical care only
- Helping someone else apply
- Not applying for yourself

Genetic Information

DHS does not collect, maintain or use genetic information for purposes of eligibility.

Record Retention

Information provided in an application for coverage through

try to recover your MA costs from your spouse's estate. However, recovery is further delayed if you still have a child who is under 21 or permanently disabled.

DHS is subject to the False Claims Act and may be kept for up to 10 years. DHS follows the general records retention schedules for state agencies and for the Department of Human Services and maintains data according to state and federal law. After the appropriate time period, DHS destroys the data in a way that prevents their contents from being determined, including by shredding paper files and permanently removing electronic data so as to prevent recovery.

Your Civil Rights

Discrimination is against the law. The Minnesota Department of Human Services (DHS) does not discriminate on the basis of any of the following: race, color, national origin, creed, religion, public assistance status, marital status, age, disability, sex (including sexual orientation and gender identity) or political beliefs.

Free Services

Auxiliary aids

If you have a disability and need aids and services to have an equal opportunity to participate in our health care programs, MNsure and DHS will provide them timely and free of charge. These aids and services include qualified interpreters and information in accessible formats.

Language assistance

If you have difficulty understanding English and need language help to access information and services, DHS will provide language assistance services timely and free of charge. These services include translated documents and interpreting spoken language.

To request these free services from DHS, call DHS Health Care Consumer Support at 651-297-3862 or 800-657-3672. Or use your preferred relay service.

Civil Rights Complaints

You have the right to file a discrimination complaint if you believe you were treated in a discriminatory way by a human services agency.

You may contact any of the following three agencies directly to file a discrimination complaint.

U.S. Department of Health and Human Services' Office for Civil Rights (OCR)

You have a right to file a complaint with the OCR, a federal agency, if you believe you have been discriminated against because of any of the following: race, color, national origin, age, disability, or sex (including sexual orientation and gender identity).

Contact the **OCR** directly to file a complaint: Centralized Case Management Operations

U.S. Department of Health and Human Services

200 Independence Avenue SW
Room 509F, HHH Building
Washington, DC 20201

800-368-1019 (voice), 800-537-7697 (TDD)

202-619-3818 (fax)

OCRComplaint@hhs.gov (email)
https://ocrportal.hhs.gov/

Minnesota Department of Human Rights (MDHR)

In Minnesota, you have the right to file a complaint with the MDHR if you believe you have been discriminated against because of any of the following: race, color, national origin, religion, creed, sex, sexual orientation, marital status, public assistance status, or disability.

Contact the **MDHR** directly to file a complaint:

Minnesota Department of Human Rights
540 Fairview Avenue North, Suite 201 St.
Paul, MN 55104
651-539-1100 (voice) or 800-657-3704 (toll free)
711 or 800-627-3529 (MN Relay)
651-296-9042 (fax)
lnfo.MDHR@state.mn.us (email)
https://mn.gov/mdhr/intake/consultationi
nquiryform/

DHS

You have a right to file a complaint with DHS if you believe you have been discriminated against in our health care programs because of any of the following: race, color, national origin, creed, religion, public assistance status, marital status, age, disability, sex (including sexual orientation and gender identity), or political beliefs.

Complaints must be in writing and filed within 180 days of the date you discovered the alleged discrimination. The complaint must contain your name and address and describe the discrimination you are complaining about. After we get your complaint, we will review it and notify you in writing about whether we have authority to investigate. If we do, we will investigate the complaint.

DHS will notify you in writing of the investigation's outcome. You have the right to appeal the outcome if you disagree with the decision. To appeal, you must send a written request to have DHS review the investigation outcome. Be brief and state why you disagree with the decision. Include additional information you think is important.

If you file a complaint in this way, the people who work for the agency named in the complaint cannot retaliate against you. This means they cannot punish you in any way for filing a complaint. Filing a complaint in this way does not stop you from seeking out other legal or administrative actions.

Contact **DHS** directly to file a

discrimination complaint: Civil Rights

Coordinator
Minnesota Department of Human Services
Equal Opportunity and Access
Division PO Box 64997
St. Paul, MN 55164-0997
651-431-3040 (voice) or use your preferred relay service.

651-431-2670 or 800-657-3739

Attention. If you need free help interpreting this document, call the above number.

ያስተውሱ፡ ካለምንም ክፍያ ይህንን ዶኩመንት የሚተረጉምሎ አስተርጓሚ ከፈለጉ ከላይ ወደተጻፈው የስልክ ቁጥር ይደውሉ።

ملاحظة: إذا أردت مساعدة مجانية لترجمة هذه الوثيقة، اتصل على الرقم أعلاه.

သတိ။ ဤစာရွက်စာတမ်းအားအခမဲ့ဘာသာပြန်ပေးခြင်း အကူအညီလိုအပ်ပါက၊ အထက်ပါဖုန်းနံပါတ်ကိုခေါ်ဆိုပါ။

កំណត់សំគាល់ ។ បើអ្នកត្រូវការជំនួយក្នុងការបកប្រែឯកសារនេះដោយឥតគិតថ្លៃ សូមហៅទូរស័ព្ទតាមលេខខាងលើ ។

請注意，如果您需要免費協助傳譯這份文件，請撥打上面的電話號碼。

Attention. Si vous avez besoin d'une aide gratuite pour interpréter le présent document, veuillez appeler au numéro ci-dessus.

Thov ua twb zoo nyeem. Yog hais tias koj xav tau kev pab txhais lus rau tsab ntaub ntawv no pub dawb, ces hu rau tus najnpawb xov tooj saum toj no.

ဟ်သူဉ်ဟ်သးဘဉ်တက္ၢါ.ဖဲနမ့ါလိဉ်ဘဉ်တါမၤစၢၤကလိလၢတါကကျိုးထံဝဲၤဉ်လ်ာတိလ်ာမီတခါအံၤန္ဉဉ်,ကိုးဘဉ်လီတဲစီနိုါဂၢ်လၢထးအံၤန္ဉဉ်တက္ၢါ.

알려드립니다. 이 문서에 대한 이해를 돕기 위해 무료로 제공되는 도움을 받으시려면 위의 전화번호로 연락하십시오.

ໂປຣດຊາບ. ຖ້າທ່ານ ທ່ານຕ້ອງການການຊ່ວຍເຫຼືອໃນການແປເອກະສານນີ້ຟຣີ, ຈົ່ງໂທຣໄປທີ່ໝາຍເລກຂ້າງເທິງນີ້.

Hubachiisa. Dokumentiin kun tola akka siif hiikamu gargaarsa hoo feete, lakkoobsa gubbatti kenname bilbili.

Внимание: если вам нужна бесплатная помощь в устном переводе данного документа, позвоните по указанному выше телефону.

Digniin. Haddii aad u baahantahay caawimaad lacag-la'aan ah ee tarjumaadda (afcelinta) qoraalkan, lambarka kore wac.

Atención. Si desea recibir asistencia gratuita para interpretar este documento, llame al número indicado arriba.

Chú ý. Nếu quý vị cần được giúp đỡ dịch tài liệu này miễn phí, xin gọi số bên trên.

LB2 (10-20)

APPENDIX II

FORM 6

REQUEST FOR DISCLOSURE OF INFORMATION

CLAY COUNTY REQUEST FOR INFORMATION
Minnesota Government Data Practices Act
(Pursuant to Clay County HIPAA Policy)

A. REQUESTOR COMPLETE (Items 1-4)

1. _____
   Date and Time of Request

2. _____ _____
   Requestor Name (last, first, MI) Telephone Number

3. Description of the Information Requested:_____
   _____

4. _____
   Signature of Requestor (if needed)

5. Proof of Identity (if data is classified private): (Picture ID, Driver's License, State ID, Student
   _____
   _____

B. DEPARTMENT USE (All requests for information shall be reviewed by the Designee of

6. Request type: ____In Person ____Mail ____Phone

7. Request handled by:_____

8. Request by: ____Subject of the Data ____Not Subject of Data

9. The information is classified: ____Public ____Private ____Confidential
   ____Non-Public ____Protected Non-Public

10. Request: ____Approved ____Denied ____Approved in Part
    (Explain in 11)

11. Action Taken: (If requested data is classified so as to deny access to the requestor, cit
    enter any remarks, comments appropriate.)
    _____
    _____

12. Supervisor or Designee Signature:_____

13. I have been permitted to inspect the data described above.

    _____ _____
    Signature of Requestor Date
    (Picture ID, Driver's License, State ID, Student ID)

APPENDIX II

FORM 7

RECEIPT FORM, COPIES OF INDIVIDUAL'S RECORDS

CLAY COUNTY

RECEIPT FORM

COPIES OF INDIVIDUAL'S PHI RECORDS

Individual's Name _____

Agency/Department _____

Description of Copies of PHI Records (e.g., client records from 1/1/2003– 1/1/2004)

_____
_____
_____
_____

I hereby acknowledge that I have received copies of the PHI records as described above:

Signature _____ **Date** _____
Printed Name_____
Client/Legal Representative Signature _____
Printed Name_____ **Date**_____

Employee Releasing Copies of Records Signature _____
Printed Name _____**Date**_____

Documents Provided to Verify Identity of the Individual Receiving the PHI Record Copies

At least one of the documents must be a photo ID **(please attach copies of the documents)**

<u>Photo Identification Provided</u> **<u>Second Form of Identification</u>**
(If there are ethnic or religious prohibitions to photographic images, you may substitute another form of identification in "Other")

- ☐ **Passport**
- ☐ **Driver's License**
- ☐ **School ID with photograph**
- ☐ **Military ID**
- ☐ **Other** _____

- ☐ **Voter's registration card**
- ☐ **Birth certificate**
- ☐ **Social Security card**
- ☐ **Credit card <u>DO NOT COPY</u> Type (e.g., Visa, Sears)**
- ☐ **Other** _____

Note: *Send Copy of this Form to Privacy Officer*

APPENDIX II

FORM 8

REQUEST FORM, AMENDMENT OF AN INDIVIDUAL'S PHI RECORDS

CLAY COUNTY

REQUEST FORM

AMENDMENT OF AN INDIVIDUAL'S PHI RECORDS

Individual's Name _____

Agency/Department _____

Description of Requested Amendment of PHI Records:

_____
_____
_____
_____

I hereby acknowledge that I have the legal authority to request amendment of records from the client record of _____ because I am the:

☐ **Individual**

☐ **Parent if client is a minor**

☐ **Court-appointed legal guardian**

☐ **Power of Attorney (financial and/or medical)**
please circle

☐ **Other** _____
e.g., Executor of Estate, etc.

Please amend my PHI as described above and include amendment in my files.

Signature _____**Date** _____
Printed Name _____

Client/Legal Representative Signature _____
Date_____ **Printed Name** _____

Employee Verifying Legal Authority to Request Amendment of PHI Records:

Signature _____**Date** _____
Printed Name _____

Note: ***Send copy to the Privacy Officer***

APPENDIX II

FORM 9

REQUESTS FOR AN ACCOUNTING OF DISCLOSURES OF HEALTH INFORMATION

CLAY COUNTY

REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF HEALTH INFORMATION

Individual's information

Name

Social Security Number

Date of Birth

Requestor's information (if not the individual)

Name

Relationship to the individual

Source of legal authority

I request that Clay County provide me with an accounting of disclosures that have been made regarding my health information for the time period identified below.

From _____, 20__, to _____, 20__.

I recognize that the Clay County will not honor a request for an accounting that extends for a period longer than six (6) years from the date the accounting is requested.

☐ I wish to receive an accounting of all disclosures made about the individual in the time frame noted above.

☐ I wish to receive an accounting of the following types of disclosures:

I understand that this accounting will not contain information pertaining to disclosures made for the following reasons:

- For treatment, payment, or healthcare operations.
- To the individual or Legal Representative.
- For use in the Clay County's individual lists or directory.
- To person's involved in the individual's care, such as family members.
- For national security purposes.
- About an inmate to correctional institutions or law enforcement officials.
- To a health oversight agency or law enforcement official for the period of time that the agency or official asked to have the information not disclosed
- Made pursuant to a written authorization by the individual or personal representative.

I understand that if this is the first accounting that I have requested in any twelve (12) month period, there will be no charge for the accounting. However, if I have made previous requests for an accounting in the last 12 months, then I will be charged the following: twenty (.20) cents per page. I understand that I may withdraw or modify this request at any time prior to the accounting being provided to me, and that if I withdraw my request prior to the Clay County acting upon it, I will not incur any charges.

I understand that the Clay County has up to ninety (90) days to respond to this request.

Signature of Requestor

Date

Printed Name

ATTN: Clay County Privacy Officer

APPENDIX II

FORM 10

REQUEST FORM, RESTRICTION ON USE OF PHI AND DISCLOSURE

CLAY COUNTY

REQUEST FORM

RESTRICTION ON USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Name: _____ Address: _____

Social Security Number: _____ _____

Date of Birth: _____ _____

Date: _____

This is a request for a restriction on Use and Disclosure of Personal Health Information. Explain the request and basis for the request: (attach additional sheets of paper if needed)

_____
_____
_____
_____
_____
_____

You will be notified by the Clay County ("Clay County") Privacy Officer if your request will be granted or denied. The Clay County Privacy Officer will act on your request as soon as administratively possible.

*__PLEASE NOTE__ that your request is governed by federal law and may be granted or denied as determined by the Clay County Privacy Officer in accordance with such law. The Clay County Privacy Officer will notify you of its decision in writing and will provide you with reasons for a denial.

I certify that I have completed, read, and understood this Request Form.

_____ _____

Requestor's Signature Printed Name Date

Deliver this form to the Clay County Privacy Officer

APPENDIX II

FORM 11

REQUEST FORM, RESTRICTION ON MANNER AND METHOD OF COMMUNICATION OF PHI

CLAY COUNTY

REQUEST FORM

RESTRICTION ON MANNER AND METHOD OF COMMUNICATION OF PROTECTED HEALTH INFORMATION

Name: _____ Address: _____

Social Security Number: _____ _____

Date of Birth: _____ _____

Date: _____

This is a request for a restriction on the manner and method of receiving confidential communications involving protected health information from Clay County ("Clay County"). Please explain the request and basis for the request: (attach additional sheets of paper if needed)

_____
_____
_____
_____
_____
_____

You will be notified by the Clay County Privacy Officer if your request will be granted or denied. The Clay County Privacy Officer will act on your request as soon as administratively possible.

*__PLEASE NOTE__ that your request is governed by federal law and may be granted or denied as determined by the Clay County Privacy Officer in accordance with such law. The Clay County Privacy Officer will notify you of its decision in writing and will provide you with reasons for a denial.

I certify that I have completed, read, and understood this Request Form.

_____ _____

Requestor's Signature Printed Name Date

Deliver this form to the Clay County Privacy Officer

APPENDIX II

FORM 12

HIPAA COMPLAINT FORM

CLAY COUNTY ("CLAY COUNTY")

HIPAA COMPLAINT FORM

Your Name:_____
Address:_____
Telephone Number:_____ Fax:_____
E-mail Address:_____ Date:_____

If you are filing a complaint on someone's behalf, provide the name and address of the person on whose behalf you are filing.

Name:_____
Address:_____

Information about Suspected Privacy Violation:

Please list the name of the Clay County staff member(s) and/or program that is suspected of a privacy violation:_____

Please describe in detail the nature of your privacy complaint, including the date or dates of the incident(s), and the name or names of any Clay County staff members involved and other witnesses (attach additional sheets if necessary):

_____

_____

_____

_____

_____

_____

Printed Name _____

Signature _____

Relationship _____

Date _____

Send to: Clay County Privacy Officer

APPENDIX II

FORM 13

HIPAA COMPLAINT RESOLUTION CHECKLIST

CLAY COUNTY

HIPAA COMPLAINT RESOLUTION CHECKLIST

- ☐ Person Filing Complaint:_____
- ☐ Date of Complaint:_____
- ☐ Case Records Involved:_____
- ☐ Nature of Complaint:_____
- ☐ Business Associate Involved?_____
- ☐ Interviews conducted:
  - A. Name and Date:_____
  - B. Name and Date:_____
  - C. Name and Date:_____
  - D. Name and Date:_____
- ☐ Describe Other Fact Finding:_____

  _____
- ☐ Facts Revealed from Investigation:_____

  _____
- ☐ Section(s) of HIPAA Policy and/or Operating Rules Implicated:_____

  _____
- ☐ Remedial Action:
  - A. Mitigate Harmful Effects
    - ☐ Was Claimant Notified?_____
    - ☐ Any other Affected Parties?_____
    - ☐ Notification to Affected Parties Needed?_____

      _____
- ☐ Additional HIPAA Training Needed? Explain:_____

_____

_____

☐ Disciplinary Action Needed?_____

Name:_____

Action:_____

_____

☐ Amendment to Privacy Policy Needed?_____

Section of Policy:_____

Proposed Amendment:_____

_____

☐ Amendment to Administrative or Internal Operations Needed?_____

_____

Cite the Specific Operating Rule and Proposed Change:_____

_____

☐ Additional Steps to Avoid Future Complaints:_____

_____

_____

Completed by:_____ Date:_____

Printed Name:_____

APPENDIX II

FORM 14

INCIDENT REPORT FORM

CLAY COUNTY

INCIDENT REPORT

Department		**Incident Location**	
Date of Incident		**Time of Incident**	
Date Reported		**Time Reported**	

UPON IDENTIFYING AN INCIDENT,

1. **Take initial steps necessary to secure/protect individuals and/or property.**
2. **Complete and send form via e-mail to Privacy Officer**
3. **Fully cooperate with the fact-finding and/or resolution process.**

INVOLVED PARTY(S):	**#1**	**#2**
Name:		
Street Address:		
City, State & Zip:		
Phone #:		

Add Additional Pages When Needed

Describe Incident:

Were there witnesses to the incident? ❑

	Witness #1		**Witness #2**
Name:		**Name:**	
Address:		**Address:**	
Tele #:		**Tele #:**	

EMPLOYEE (COMPLETE)

CORRECTIVE ACTION TAKEN:

OTHER COMMENTS:

RECOMMENDED FOR FURTHER REVIEW BY:

SIGNATURE/DATE **PRINT NAME**

SUPERVISOR (COMPLETE)

CORRECTIVE ACTION TAKEN/RECOMMENDED:

APPENDIX II

FORM 15

MODEL BUSINESS ASSOCIATE AGREEMENT

ADDENDUM TO AGREEMENT/CONTRACT WITH CLAY COUNTY

This Addendum is made part of the Agreement by and between **Clay County Social Services** (Agency) and …….(Business Associate).

Agency and Business Associate agree to modify the Agreement, in order to comply with the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as set forth in Title 45, Parts 160 and 164 of the Code of Federal Regulations (the "CFR"). In the event of conflicting terms or conditions, this Addendum shall supersede the Agreement.

1. **Definitions**. Capitalized terms not otherwise defined in the Agreement shall have the meanings given to them in Title 45, Parts 160 and 164 of the CFR and are incorporated herein by reference.

2. **Use and Disclosure of Protected Health Information**. Business Associate shall use and/or disclose Protected Health Information ("PHI") only to the extent necessary to satisfy Business Associate's obligations under the Agreement consistent with Agency's minimum necessary policies. To the extent Business Associate is to carry out one or more of Agency's obligation(s) under Subpart E of 45 CFR Part 164, it shall comply with the requirements of Subpart E that apply to Agency in the performance of such obligation(s).

3. **Prohibition on Unauthorized Use or Disclosure of PHI**. Business Associate shall not use or disclose any PHI received from or on behalf of Agency, except as permitted or required by the Agreement, as required by law or as otherwise authorized in writing by Agency. Business Associate shall comply with: (a) Title 45, Part 164 of the CFR; (b) State laws, rules and regulations applicable to PHI not preempted pursuant to Title 45, Part 160, Subpart B of the CFR; and (c) Agency's health information privacy and security policies and procedures (collectively "Applicable Law").

4. **Business Associate's Operations**. Business Associate may use PHI it creates or receives for or from Agency only to the extent necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities. Business Associate may disclose such PHI as necessary for Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities only if:

   (1) The disclosure is required by law; or
   (2) Business Associate obtains reasonable assurance, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:
      (a) Hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization or as required by law; and
      (b) Notify Business Associate (who shall in turn promptly notify Agency) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached.

5. **PHI Safeguards**. Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical safeguards to prevent the improper use or disclosures of any PHI received from or on behalf of Agency.

6. **Electronic Health Information Security and Integrity**. Business Associate shall develop, implement, maintain and use appropriate administrative, technical and physical security measures in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320d-2(d) of the United States Code, Title 45, Part 142 of the CFR, and other Applicable Law to preserve the integrity and confidentiality of all electronically maintained or transmitted Health Information received from or on behalf of Agency pertaining to an Individual. Business Associate shall document and keep these security measures current.

7. **Protection of Exchanged Information in Electronic Transactions**. If Business Associate conducts any Standard Transaction for or on behalf of Agency, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the CFR. Business Associate shall not enter into or permit its subcontractors or agents to enter into any Trading Partner Agreement in connection with the conduct of Standard Transactions for or on behalf of Agency that: (a) changes the definition, Health Information condition or use of a Health Information element or segment in a Standard; (b) adds any Health Information elements or segments to the maximum defined Health Information set; (c) uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification or are not in the Standard's Implementation Specification(s); or (d) changes the meaning or intent of the Standard's Implementation Specification(s).

8. **Subcontractors and Agents**. Business Associate shall require each of its subcontractors or agents to whom Business Associate may provide PHI received from, or created or received by Business Associate on behalf of Agency to agree to

written contractual provisions that impose at least the same obligations to protect such PHI as are imposed on Business Associate by the Agreement.

9. **Access to PHI**. Business Associate shall provide access, at the request of Agency, to PHI in a Designated Record Set, to Agency or, as directed by Agency, to an Individual in order to meet the requirements under Title 45, Part 164, Subpart E, Section 164.524 of the CFR and applicable State law. Business Associate shall provide access in the time and manner set forth in Agency's health information privacy and security policies and procedures.

10. **Amending PHI**. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Agency directs or agrees to pursuant to Title 45, Part 164, Subpart E, Section 164.526 of the CFR at the request of Agency or an Individual, and in the time and manner set forth in Agency's health information privacy and security policies and procedures.

11. **Accounting of Disclosures of PHI**. (1) Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Agency to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Part 164, Subpart E, Section 164.528 of the CFR. (2) Business Associate agrees to provide Agency or an Individual, in time and manner set forth in Agency's health information privacy and security policies and procedures, information collected in accordance with Section 11 (a) above, to permit Agency to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with Title 45, Part 164, Subpart E, Section 164.528 of the CFR.

12. **Access to Books and Records**. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from or on behalf of Agency available to Agency and to DHHS or its designee for the purpose of determining Agency's compliance with the Privacy Rule.

13. **Reporting**. Business Associate shall report to Agency any use or disclosure of PHI not authorized by the Agreement or in writing by Agency, including incidents that constitute any breach of unsecured PHI as required under 45 CFR 164.410, and any security incident of which it becomes aware. Business Associate shall make the report to Agency's Privacy Official not less than 24 hours after Business Associate learns of such unauthorized use or disclosure. Business Associate's report shall at least: (a) identify the nature of the unauthorized use or disclosure; (b) identify the PHI used or disclosed; (c) identify who made the unauthorized use or received the unauthorized disclosure; (d) identify what Business Associate has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; (e) identify what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure; and (f) provide such other information, including a written report, as reasonably requested by Agency's Privacy Official.

14. **Mitigation**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of the Agreement.

15. **Termination for Cause**. Upon Agency's knowledge of a material breach by Business Associate, Agency shall: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate if Business Associate does not cure the breach or end the violation within the time specified by Agency. (2) Immediately terminate the Agreement if Business Associate has breached a material term of the Agreement and cure is not possible. (3) If neither termination nor cure is feasible, Agency shall report the violation to the Secretary.

16. **Return or Destruction of Health Information**. (1) Except as provided in Section 16(b) below, upon termination, cancellation, expiration or other conclusion of the Agreement, Business Associate shall return to Agency or destroy all PHI received from Agency, or created or received by Business Associate on behalf of Agency. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. (2) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Agency notification of the conditions that make return or destruction infeasible. Upon verification by Agency that the return or destruction of PHI is infeasible, Business Associate shall extend the protections of the Agreement to such PHI and limit further uses and disclosure of PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

17. **Automatic Amendment**. Upon the effective date of any amendment to the regulations promulgated by DHHS with respect to PHI, the Agreement shall automatically amend such that the obligations imposed on Business Associate as a Business Associate remain in compliance with such regulations.